NEW TECHNIQUES FOR QUANTUM COMMUNICATION SYSTEMS

A Thesis
Presented to
The Academic Faculty

by

Zheshen Zhang

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
December 2011

NEW TECHNIQUES FOR QUANTUM COMMUNICATION SYSTEMS

Approved by:

Professor Abdallah Ougazzaden,
Committee Chair
School of Electrical and Computer
Engineering
Georgia Institute of Technology

Professor Paul L. Voss, Advisor
School of Electrical and Computer
Engineering
Georgia Institute of Technology

Professor David S. Citrin
School of Electrical and Computer
Engineering
Georgia Institute of Technology

Professor Matthieu Bloch
School of Electrical and Computer
Engineering
Georgia Institute of Technology

Professor Andrew Zangwill
School of Physics
Georgia Institute of Technology

Date Approved: 07 November 2011

To my family.

ACKNOWLEDGEMENTS

I am grateful to my advisor, Dr. Paul Voss, for his patient guidance during the past five years. Dr. Voss possesses not only a deep understanding in the area of quantum communication and nonlinear optics, but also an extremely broad range of knowledge of science, history, economics, and politics. Dr. Voss's enthusiasm and curiosity always lead to new ideas and open up new possibilities. I have also been fortunate to work with friendly, bright, and collaborative people in my lab. I not only spent some agreeable time with Quyen on the quantum key distribution project, but also shared happiness with his family. I enjoy working in the lab with Nicolas, an expert in optical experiments as well as racing, tennis, and golf. Olivier always unconditionally supports our experiments by his expertise in electronics. He is also my French teacher, under whose instructions my French achieved tremendous progress. I have had some pleasant discussions on science, philosophy, and culture with Mahbub, a new PhD student in the lab since the beginning of this year. Finally, I would like to thank Dr. Walt de Heer's group for providing epitaxial graphene samples for our graphene four-wave mixing experiment.

I also would like to mention some other people who did not collaborate with our research group. Wui-hean, the first Chinese-speaking person I have known in France, has been a friend for five years since our first meet on the orientation day of Fall 2006. Jingfei, a Chinese PhD student who came later, always helps me with my life. Peter is a regular guest to my kitchen, and we made some memorable trips with his old nevertheless pretty car"Madame Peugeot". Fred, Audrey, Vinod, Constantinos, and Mohammed actively make a lively atmosphere in the PhD office, leading to many of jokes and laughs.

I wish to express my gratefulness to the staff at GTL. I really appreciate Josyane for her continuous help for my residence cards, my visas, my insurance, and even my bank problems. Jean-Jacque is able to solve all kinds of strange and complicated computer problems. With his efforts, everyone at GTL benefits from a stable network. Sandrine, a nice lady who loves Chinese culture, makes our equipment orders fast and efficient. Christine is a "gentille" cleaning lady who is friendly to everyone at GTL and likes making French jokes. I especially benefit from her efforts to make the lab tidy and organized.

Last but not least, I would like to acknowledge continuous spiritual support from my family. It gives me confidence, encouragement, motivation, and faith to finish my PhD work and to dedicate myself to science.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

The emergence of the Internet enables global communications, which quickly transmits information from any place in the world to any another place in the world. The entire chain of global communications consists of three components: information processing, information communication, and information storage. In the information processing phase, information from various sources is distilled, combined, and transformed locally. The processed information is then transmitted from one place to another via an information communication phase. In the information storage phase, information is recorded into storage media for future use. As a result, the performance of global communications is determined by the performance of individual singular subsystems. Moore's law predicts a long-term trend of the performance of information processing. According to Moore's law [1], the number of transistors that can be integrated into a unit area of circuit doubles every 18 months. Moore's law leads to predictions of exponential increase in information-processing performance and decrease in unit cost. Although Moore's law was first described in the 1960s, it is still valid thanks to continuous innovations in the semi-conductor industrial. On the other hand, novel technologies such as fiber communications, wireless communications, and satellite communications are widely applied to allow high-rate communication and flexible access to the Internet. For information storage, large-volume hard disks, high-density optical storage devices, and solid-state disks were invented, leading to large-capacity and high-reliability information storage.

Continuous performance improvements of global communications do not always

meet the needs of people. For certain applications, information must be communicated not only efficiently, but also confidentially. Cryptography is a subject dealing with secure communication. Widely-used mathematical cryptography is constructed on the application layer, where mathematical encryption and decryption algorithms are carefully designed and implemented. The security of mathematical cryptography relies on mathematical problems that are assumed to be hard to solve. Physical-layer security an alternative method that makes use of physical noise processes instead of unproven mathematical assumptions to guarantee the security of communication. In the following sections, we will discuss in detail some limitations of mathematical cryptography, advantages of physical-layer security, bottlenecks of current implementations of physical-layer-security, and useful techniques that potentially lead to more efficient and lower-cost physical-layer-security systems. This discussion thus provides a conceptual framework to explain the significant of the research reported in this thesis.

1.1 Limitations of conventional cryptography

Two primary demands for secure communication are strong security and fast processing time. However, different secure-communication systems are limited by, one way or another, technical limitations. In this section, technical difficulties for both mathematical cryptography and physical-layer security will be discussed. Knowing the technical difficulties, unsolved problems in current secure-communication systems can be identified.

Public-key mathematical cryptography is widely applied in the Internet. The security of public-key mathematical cryptography is based on mathematical problems such as the discrete-logarithm problem, the large-number factoring problem, the subset-sum problem, and the multivariate-quadratic problem [2]. Given a solution of one of these problems, one only needs an amount of time that is a polynomial

function of the input size to verify the correctness of the solution. However, to find solutions of such problems, only algorithms with super-polynomial time complexity are known. The best known factoring algorithm is " the general number field sieve", with time complexity $O\left(\exp\left(\left(\frac{64}{9}b\right)^{\frac{1}{3}}\log(b)^{\frac{2}{3}}\right)\right)$ [3], where b the size in bits of the integer to factor. Such difficult mathematical problems are basic units for construction of one-way functions, which are easy to evaluate but hard to invert. The existence of one-way functions would resolve the "P $\neq$ NP" assertion [4], which has been the largest unsolved problem for the computer-science community for over 40 years. During this time computer scientists have made little progress towards proving either "P = NP" or "P $\neq$ NP". In essence, the "P = NP" problem asks whether all problems which can be verified in polynomial time can also be solved in polynomial time. Several well-known results [5, 6] show surprisingly high barriers towards proving"P $\neq$ NP". In summary, relativizing proofs [5] (based on fixed subroutines) and natural proofs [6] (based on circuit complexity lower bounds) cannot help proving with the "P = NP" problem. As a result, a provable super-polynomial lower bound for the time complexity still seems to be very unrealistic given the state of the art of the computational-complexity research.

In practice, people have also launched attacks against current mathematical cryptosystems. For private-key cryptosystems, although the old DES standard has been recently replaced by the AES standard to strengthen security, new attacks against AES have already been proposed [7], revealing weaknesses in the security of AES. For public-key cryptosystems, algorithms based on the factoring problem are vulnerable to a quantum algorithm that is able to exponentially decrease the time complexity of finding a solution [8]. The advent of quantum computers would break the security of current public-key cryptosystems.

1.2 Physical-layer security

To circumvent potential security weaknesses of mathematical cryptography, one can implement secure-communication systems based on other principles. Physical-layer security provides such an alternative. Physical-layer security relies on the physical properties of nature instead of unproven mathematical assumptions. Compared to mathematical cryptography, physical-layer security is provable without resorting to mathematical assumptions. Next, let us discuss a typical model for physical-layer security in order to illustrate. We assume that two legitimate users, i.e., Alice and Bob, share a communication channel with a certain signal to noise ratio. An eavesdropper, who we shall call Eve, is listening to the transmissions between Alice and Bob on the channel. If Eve's channel is not perfect, Eve's knowledge of the transmitted signal between Alice and Bob is contaminated by noise. The quality of Eve's channel thus sets a limit on Eve's capability of estimating messages transmitting in the communication channel. In particular, the security of communication can be measured by the secrecy capacity of the channel [9], which will be defined rigorously in the context of this thesis.

Physical-layer security has been theoretically proven and experimentally implemented for quantum key distribution (QKD) systems [10]. The advantage of using quantum states for communication is that security can be guaranteed by physical laws in quantum mechanics, in particular, the quantum uncertainty principle and the quantum no-cloning theorem. This is true even if Eve has any realizable apparatus. By performing quantum measurements, Alice and Bob are able to bound Eve's accessible information and thus achieve unconditional security. However, as we will discuss in the context of this thesis, QKD only guarantees the main channel security, where Eve is not able to capture any information of the generated key from the quantum channel or the public authenticated classical channel. Eve can still launch side-channel attacks in which Eve tries to monitor power-level changes or break the

random-number generator used by Alice and Bob.

Physical-layer security has also been introduced for wireless communication systems [11]. To achieve secure communication, a positive secrecy capacity is desired. Unlike the security of QKD, which can be quantified and deduced through experimental quantum measurements, the security of wireless communication systems can be estimated by making assumptions on what the eavesdropper can do. Reasonable assumptions on Eve's channel quality lead to mathematically provable security, which is valid if the channel model holds.

The rate of physical-layer security is slow compared to conventional mathematical cryptography. In practice, the combination of physical-layer security and conventional mathematical cryptography leads to reasonable security and high rate. For example, QKD solves the key distribution problem and normal block ciphers are used for encryption.

1.3 Useful techniques for physical-layer security

Implementations of physical-layer security need various technical supports. For example, QKD systems need large amount of random numbers for quantum-state selection and measurement-basis switching. Random numbers used in QKD need to be truly random to validate security proofs. For high-rate QKD experiments, ultrafast random-number generators working at GHz rates are desired. On the other hand, true random numbers are also desired in mathematical cryptosystems such as the ElGamal encryption system [12]. Another useful technique for physical-layer security is quantum-entanglement production. Many QKD protocols require quantum entangled states to carry quantum information [13]. Quantum entanglement is also essential for other quantum-communication applications such as quantum teleportation [14], which is of great importance for the proposed quantum internet [15].

1.3.1 Physical random-number generator

Physical random-number generators make use of uncertainty in nature as a source of randomness. Many physical phenomena can be used to generate random numbers. In [16], the photon statistics at the output of beam splitter are used as a randomness source. Gated single photons arriving at In-GaAs photodiodes are measured in [17] to generate random numbers. Alternatively, random-number generators based on photon counting [18–21] are built. Other quantum-mechanical phenomena are also used to generate random numbers. For example, electron spin is a potential randomness source [22].

For random-number-generation schemes based on photon counting, the generation rate is typically limited by the bandwidth of single-photon counters. To overcome the bottleneck imposed by detector bandwidth, some other schemes are proposed. Randomness from laser phase noise caused by spontaneous emission is utilized in [23], making the replacement of single-photon counters by high-bandwidth PiN diodes possible. Quantum vacuum noise is also a potential source to generate truly random numbers [24,25]. To extract the randomness from vacuum noise, balanced homodyne detectors are required. Other candidates for physical randomness source include chaotic laser [26,27] and thermal noise in superconductive single-flux quantum circuit [28].

On the other hand, although quantum randomness has been proven to be incomputable [29], it is still important to evaluate extractable randomness from sources so that no pseudo randomness is generated. A quantum tomographic method is proposed in [30] to measure a lower bound on the minimal entropy of randomness sources. Knowing this lower bound guarantees that one does not extract more randomness than what really exists. A check can be performed by statistical tests. These tests are performed and analyzed in [31], for example. Passing statistical tests is a necessary, though not sufficient, condition for a true random-number generator.

Extractable randomness also depends on physical implementations. For example, for random-number generation schemes based on beam splitter [16], additional conditions need to be satisfied to guarantee the randomness [32].

1.3.2 Quantum entanglement generation

Quantum entanglement is one the most astonishing consequences that quantum mechanics predicts. Two entangled quantum subsystems, however far away they are separated, can still be correlated. If we make a quantum measurement on one subsystem, the quantum state of the other subsystem will be changed instantaneously by the measurement outcome.

Quantum entanglement plays a crucial role in quantum communication. Quantum entanglement is required for quantum teleportation [14], in which an arbitrary unknown quantum state can be transferred from one quantum system to another without transferring the quantum state on any quantum channel. For quantum networks [15] in the future, stable and low-complexity entanglement sources are desired. A widely applied technique to generate quantum entanglement is based on parametric down conversion (PDC) in $\chi^{(2)}$ crystals [33–35]. High efficiency and brightness are achievable for such entanglement sources while the main limitation is the coupling efficiency to practical communication systems, e.g., optical-fiber networks.

To overcome the coupling problem, nonlinear optical waveguides integrable with optical fibers are proposed as entanglement sources for optical communication [36]. To settle the phase-matching problem arising in optical fiber, quasi-phase-matching schemes are proposed. In a quasi-phase-matching scheme, optical waveguides are periodically poled with lithium niobate (PPLN) [37, 38] or orientation-patterned gallium arsenide [39]. Several experiments making use of nonlinear waveguide devices are demonstrated [40, 41].

Besides $\chi^{(2)}$ nonlinear crystals and waveguides, optical fiber has also been shown

to be a very good entanglement source at 1550 nm telecom band [42]. Entangled photons can be generated by four-wave mixing in optical fibers [43, 44].

1.4 Quantum communication architecture

In quantum key distribution, quantum states need to be communicated on a quantum channel. For quantum teleportation, although no real quantum states are transmitted through quantum channels, the purpose is still to send quantum states from one place to another by means of quantum entanglement and classical communication. Both situations belong to areas of quantum communication. Like classical communication network, quantum communication can be divided into several layers, which are illustrated in Figure 1.

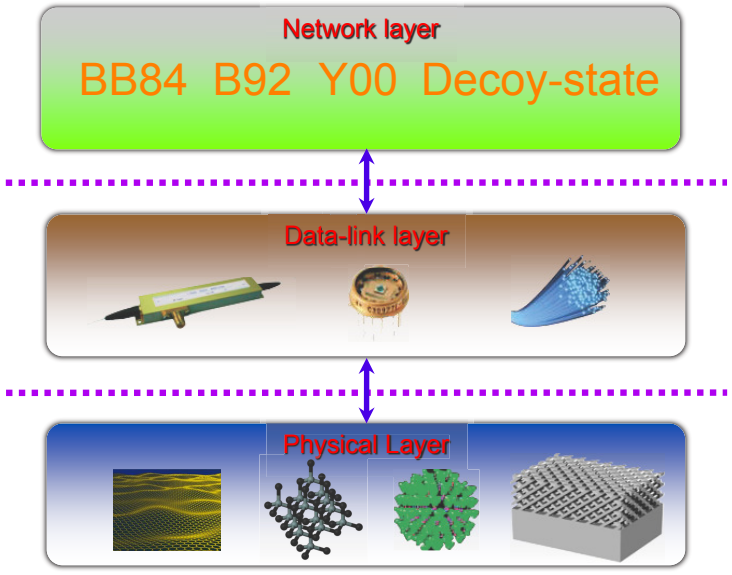


Figure 1: A typical architecture for quantum communication.

The lowest layer is the physical layer, which is composed of basic materials such as semi-conductors and atoms. These materials are the most fundamental elements to construct the entire quantum-communication network. Physical properties such as conductivity, optical linear and nonlinear response, and electronic behaviors of these materials need to be understood.

The middle layer is the data-link layer. In the data-link layer, we fabricate devices to enable the sending and the receiving of quantum signals. To send information, we usually use single-photon emitters or weak coherent lasers to produce quantum signals. To encode information onto these quantum signals, we need modulators. To transmit quantum signals, a quantum channel is required. For long distance quantum communication, optical fibers are usually employed as the quantum channel. At the receiving side, photodetectors are used. Depending on the type of quantum information, we either need PiN photodiodes or single-photon counters to perform quantum measurements. To fabricate these devices, we need knowledge on the physical properties of materials in the physical layer. Based on these devices, we can implement quantum communication systems such as quantum key distribution or quantum teleportation experiments.

The highest layer is the network layer. In the network layer, we use different quantum communication protocols to allow secure key generation in quantum key distribution or quantum state transmission in quantum teleportation. Quantum key distribution protocols are important because they not only influence the security of communication, but also have an impact on the key generation rate. The three levels are not independent. Once we design a protocol in the network layer, we need to take into account the performance limits of devices in the data-link layer. Additionally, to fabricate a device, we need to fully understand the physical properties of materials in the physical layer.

1.5 Problems to be addressed in this thesis

Thanks to its provable security, physical-layer security is superior over mathematical cryptography from a security point of view. However, throughputs of physical-layer-security based systems are much lower than mathematical cryptosystems because of technical limitations. Experimentally, two kinds of implementations of QKD systems

exist. The first kind is based on discrete-variable quantum communication, which uses single-photon counters for detection. The bandwidth of single-photon counters is bottlenecked by the recovery time of detectors. The other kind of QKD is based on continuous-variable quantum communication using PiN diodes for detection. The bandwidth of PiN diodes can be several GHz, much higher than single-photon counters. However, the bottleneck of continuous-variable quantum communication is the complexity of error-correction codes. To achieve a positive secret-key capacity for continuous-variable based QKD systems, error-correction codes are required to operate very close to the Shannon limit on large block sizes, leading to use of highly efficient error-correction codes with high complexity.

Another potential problem of high-rate QKD systems is the demand for high-speed true random-number generators used for signal selection and measurement-basis switching. True randomness to be used in signal selection and basis-switching is of great importance for security proofs because use of pseudo-random-number generators ties the security back to unproven mathematical assumptions.

A state-of-the-art key-generation rate for continuous-variable QKD system is 2.2 kbits/s [45] on a 25 km fiber link. This key-generation rate needs to be improved to match practical communication rate, which is expected to be on the order of Gbits/s. QKD systems with high key-generation rate and low cost are desired. As discussed above, QKD key-generation rate is limited by random-number generation, detection bandwidth, and/or error-correction complexity. For random-number generation, one needs to develop ultrafast true random-number generators, excluding use of any pseudo-random-number generators. True random-number generators based on quantum phenomena are called quantum random-number generators, whose design requires careful analysis of the quantum phenomena as sources and experimental proposal compatible with current technologies.

To overcome the detection-bandwidth limitation, PiN diodes can be used thanks

to their high bandwidth. From the experimental point of view, new experimental schemes need to be developed to benefit from the high-bandwidth PiN diodes. From the reconciliation point of view, we need to decrease the time complexity of error-correction codes by introducing new continuous-variable QKD protocols.

Quantum entanglement can improve quantum-communication distances and be utilized in QKD protocols. Quantum entanglement sources are nonlinear optical interactions in matter. Potential nonlinear processes for producing quantum entanglement include parametric down conversion (PDC) and four-wave mixing (FWM). To generate entanglement, we first need materials with high nonlinear susceptibility, either $\chi^{(2)}$ for PDC or $\chi^{(3)}$ for FWM. Second, we need to carefully choose the working wavelengths so that the phase-matching condition can be satisfied. It is however not easy to meet the nonlinear susceptibility and the phase-matching conditions simultaneously.

Recently, a new material, graphene, was discovered. Graphene is a monolayer of sp^2-bonded carbon atoms grown on a honeycomb crystal lattice. Graphene can be grown epitaxially on a SiC substrate [46] for convenient micro-fabrication. Graphene possesses many unusual optical properties, which makes it a very promising material for entanglement production. In this thesis, nonlinearity of graphene will be examined theoretically and a four-wave mixing experiment in graphene will be investigated.

1.6 Outline of the thesis

This thesis includes my Ph.D research work on the three layers of quantum communication architecture. An overall representation of thesis contributions is illustrated in Figure 2. In Chapter 2, preliminary theoretical knowledge will be introduced. The knowledge covered in this chapter is useful within the context of the following chapters. Chapter 3 will focus on the network layer with a proposal of a novel continuous-variable QKD protocol. The security of the proposed QKD protocol will

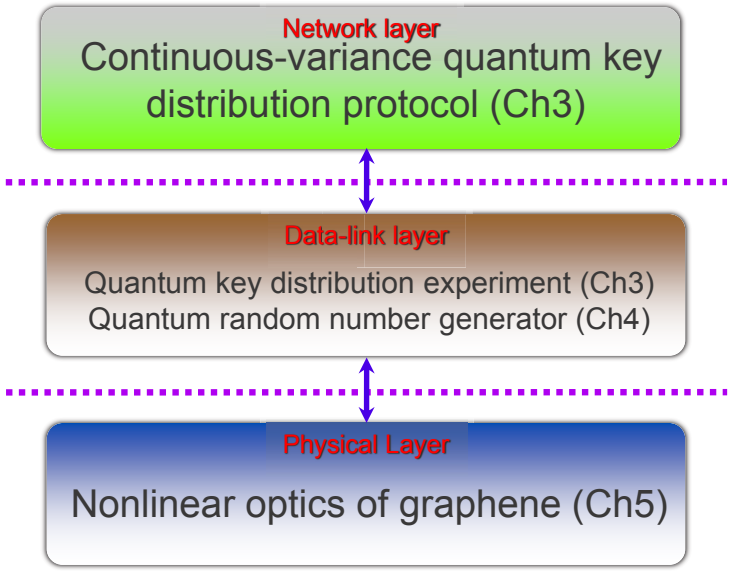


Figure 2: An overall representation of thesis contributions.

be analyzed in detail. The second part of Chapter 3 will enter into the data-link layer by introducing an experimental demonstration of the proposed QKD protocol. Chapter 4 describes an experimental implementation and theoretical study of an ultrafast quantum random-number generator based on amplified spontaneous emission. In Chapter 5, we will turn our attention to the physical layer. We will discuss the nonlinear optics of graphene, a novel material with unconventional electronic and optical properties. The content in this chapter includes both theoretical treatment on nonlinear optical processes in graphene and experimental work towards verification of the developed theory and its eventual use in quantum communications.

CHAPTER II

THEORETICAL PRELIMINARIES

This chapter introduces the preliminaries of quantum information theory, quantum optics, and nonlinear optics, which will later become useful theoretical tools within the context of this thesis. We start with classical information theory, focusing on its application to communications and security. Quantum information theory, the quantum counterpart of classical information theory, will be discussed in Sec. 2.2. Important results such as the Holevo theorem are the main topics of that section. Sec. 2.3 covers basic concepts of quantum optics. The first part of this section introduces the quantization of the electromagnetic field, which gives rise to quantum states such as the Fock state and the coherent state. These states are of great importance to quantum information. In Sec. 2.4, we will turn our attention to nonlinear optics, the key to understand optical processes such as four-wave mixing.

2.1 Classical information theory

Although information had been a commonly used word for hundreds of years, its formal mathematical definition did not emerge until the original work of Shannon in the 1940s. Shannon's work, which was later named information theory, led to profound results in communication and security. The most important accomplishment of information theory is that it finds fundamental limits on communication. Fundamental results by information theory set limits on the data-compression rate. In addition, information theory gives upper bounds for reliable communication. In particular, information theory answers the question: on a noisy channel, how much information can be reliably transferred per channel use on average. In this section, general results of information theory will be discussed. Although the results in this

section are derived from the classical point of view by assuming that quantum effects are too weak to have any practical impact on the situation of interest, understanding the ideas in this section forms the foundation for further development of quantum information theory in next section.

2.1.1 Classical entropy and mutual information

Before introducing the formal mathematical definition of information, let us consider the following two claims:

- Tomorrow is going to rain.
- Tomorrow there will be an earthquake.

If we ask ourselves which claim gives more information, our intuition tells us that the second one does because it is a less probable event to occur. This simple example illustrates that the amount of information contained in an event is a function of its probability of occurrence. We then make this statement more abstract by producing an axiomatic construction of information and entropy. Assume a random variable X, which takes values on a set $\mathcal{X} = \{x_1, x_2, ..., x_n\}$. The information obtained by learning $X = x_i$ is a function of the probability of X being x_i:

$$I(X = x_i) = f[p(x_i)]. \tag{2.1.1}$$

Our next goal is to find a specific form for f. Suppose another random variable Y taking values on the set $\mathcal{Y} = \{y_1, y_2, ..., y_n\}$ is independent of X. It is reasonable to let the information obtained by learning $X = x_i$ and $Y = y_j$ be the sum of the information obtained by learning each independent event. Mathematically, we have

$$\begin{aligned} I(X = x_i \text{ and } Y = y_j) &= f[p(x_i, y_j)] \\ &= I(X = x_i) + I(Y = y_j) \\ &= f[p(x_i)] + f[p(y_j)]. \end{aligned} \tag{2.1.2}$$

Since X and Y are independent random variables, the probability for both events to occur is the product of the probability of the occurrence of each single event. Thus, we have

$$p(x_i, y_j) = p(x_i) \cdot p(y_j). \tag{2.1.3}$$

Substituting Eq. 2.1.3 into Eq. 2.1.2 yields

$$f[p(x_i) \cdot p(y_j)] = f[p(x_i)] + f[p(y_j)]. \tag{2.1.4}$$

Eq. 2.1.4 implies that f is in a logarithm form. Furthermore, since $p(x_i) \leq 1$, and non-negative values are required to represent information, we define the information obtained by learning $X = x_i$ as

$$I(X = x_i) = -\log_k[p(x_i)], \tag{2.1.5}$$

where k is the logarithmic base, specifying the information unit. The information unit is *nat* for the natural logarithm and *hartley* for the common logarithm. The most common information unit is *bit*, by using $k = 2$ as the logarithmic base.

Eq. 2.1.5 defines the amount of information obtained by learning $X = x_i$. Since X is a random variable, the *average* amount of information contained in X is defined as the *entropy* of X:

$$H(X) \equiv \sum_{x \in \mathcal{X}} p(x) I(x) = \sum_{x \in \mathcal{X}} -p(x) \log p(x). \tag{2.1.6}$$

Eq. 2.1.6 defines the entropy of a single random variable X. For n random variables $X_1, X_2, ..., X_n$, the *joint entropy* is defined as

$$H(X_1, X_2, ...X_n) \equiv \sum_{x_1, x_2, ..., x_n} -p(x_1, x_2, ..., x_n) \log p(x_1, x_2, ..., x_n), \tag{2.1.7}$$

where $p(x_1, x_2, ..., x_n)$ is the joint probability distribution. The joint entropy quantifies the amount of information obtained by learning an unknown set of random variables. If the value of Y is given, the remaining entropy of X is defined as the entropy of X

conditional on Y, or simply

$$\begin{aligned} H(X|Y) &\equiv \sum_{y\in\mathcal{Y}} p(y)H(X|Y=y) \\ &= \sum_{y\in\mathcal{Y}} p(y) \sum_{x\in\mathcal{X}} -p(x|y)\log p(x|y) \\ &= \sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}} -p(x,y)\log p(x|y). \end{aligned} \tag{2.1.8}$$

One important property of the conditional entropy is its relation to the joint entropy, which is known as the chain rule:

$$\begin{aligned} H(X,Y) &= H(X) + H(Y|X) \\ &= H(Y) + H(X|Y). \end{aligned} \tag{2.1.9}$$

Eq. 2.1.9 can be proven following the mathematical definition of the entropy in Eq. 2.1.6 and the joint entropy in Eq. 2.1.7. Intuitively, the total amount of information contained in the combined random variable (X,Y) is the sum of two parts. The first part only includes the amount of information contained in one single random variable X (or Y) , calculated as $H(X)$ (or $H(Y)$). The second part includes the amount of the remaining information on the other random variable given the value of the first, yielding $H(Y|X)$ (or $H(X|Y)$).

Having defined the entropy and the joint entropy, we define the *mutual information*, an important concept in information theory. The mutual information, $I(X;Y)$, is the information on X by learning another random variable Y. If X and Y are independent, learning Y does not help to gain any information on X. However, if X and Y are perfectly correlated, $I(X;Y) = H(X)$. Thus, the mutual information $I(X;Y)$ depends on the entropy $H(X)$ as well as the correlation between X and Y. Our intuition invites us to give the following definition for $I(X;Y)$:

$$I(X;Y) \equiv H(X) - H(X|Y). \tag{2.1.10}$$

The first term of the right-hand side is the entropy of X. The second term of the right-hand side is the remaining entropy of X giving the value of Y. If X and Y

are independent, $H(X|Y) = H(X)$ results in $I(X;Y) = 0$, meaning that learning Y does not help to obtain information on X. If X and Y are completely correlated, $H(X|Y) = 0$ leads to $I(X;Y) = H(X)$, which also matches our previous discussion.

By using Eq. 2.1.9, Eq. 2.1.10 can be reorganized into

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(X,Y) \\ &= H(X,Y) - H(Y|X) - H(X|Y). \end{aligned} \tag{2.1.11}$$

The symmetry on X and Y in Eq. 2.1.11 illustrates that the amount of information on X by learning Y is equal to the amount of information on Y by learning X.

2.1.2 Channel capacity and secure communication

For the purpose of communication, messages need to be sent by a transmitter through a communication channel and observed by a receiver. In practice, communication channels usually introduce additional noise, resulting in distortions to the messages being received. Figure 3 illustrates a typical model for communication.

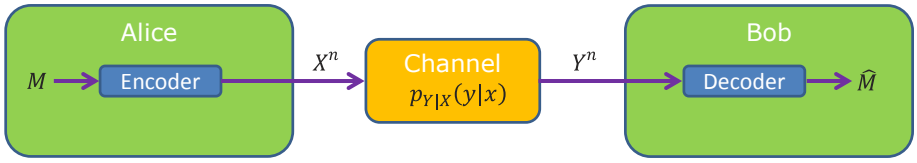


Figure 3: A typical model for communication. M **is the message to be sent.** $\hat{M}$ **is Bob's estimated message. The noise property of the channel is quantized by the conditional probability distribution** $p_{Y|X}(y|x)$**.**

If the noise properties of the channel are priorly given, information theory finds the maximum amount of information that can be transmitted reliably per channel use on average. This upper bound is defined as the *channel capacity*. Let $\mathcal{M}$ be a set of possible messages to be sent, $\mathcal{X}$ be a set of possible signals to be transmitted through the channel, and $\mathcal{Y}$ be the set of possible observed signals. The sender, Alice, first uses an encoder to convert message M drawing from the set

$$\mathcal{M} = \{1, 2, ..., 2^k\}$$

into a signal $X^n = \{x_1, x_2, ..., x_n\}$. Each x_i is a generic element in the signal alphabet $\mathcal{X}$. For the code we use, to encode k bit of information, we need n symbols. The code rate is defined as

$$R = \frac{k}{n}. \tag{2.1.12}$$

The encoded message is transmitted through a noisy channel characterized by the conditional probability distribution $p_{X|Y}(x|y)$. The receiver, Bob, feeds the observed signal Y^n to a decoder, yielding the output $\hat{M}$ to be the guess of the original message M. According to information theory, channel capacity can be found by [47]

$$C \equiv \sup_{p_X} I(X;Y). \tag{2.1.13}$$

The conversion from the original message to the transmitted signal forms a code. Shannon proved that for any $\varepsilon > 0$, $R < C$, and for large enough N, there exists a code of length N, rate $\geq R$, and a decoding algorithm such that $\text{Prob}(\hat{M} \neq M) \leq \varepsilon$.

Under certain circumstances, Alice and Bob wish to communicate in a secure manner. An eavesdropper, usually called Eve, tries to listen to the data transmitting on the channel and figure out the original message M. If Eve observes the exact copy of the signal as Bob does, any guess by Bob on the original message M can be duplicated by Eve, and there does not exist any security on the channel. However, if Bob and Eve possess different channels with different noise properties, the situation changes. Our intuition tells us that if Eve's channel is noisier than Bob's channel, Bob receives a better signal than she does, and thus secure communication between Alice and Bob is possible. The wiretap channel [47] illustrated in Figure 4 models this situation.

The noise property of a wiretap channel is modelled by the conditional probability distribution $p_{Y,Z|X}(y, z|x)$. For the purpose of secure communication, Alice and Bob use a code with code rate R to convert message $M \in \mathcal{M} = \{1, 2, ..., 2^{nR}\}$ and a random number R_X from Alice's local randomness source into signal $X^n = \{x_1, x_2, ..., x_n\}$,

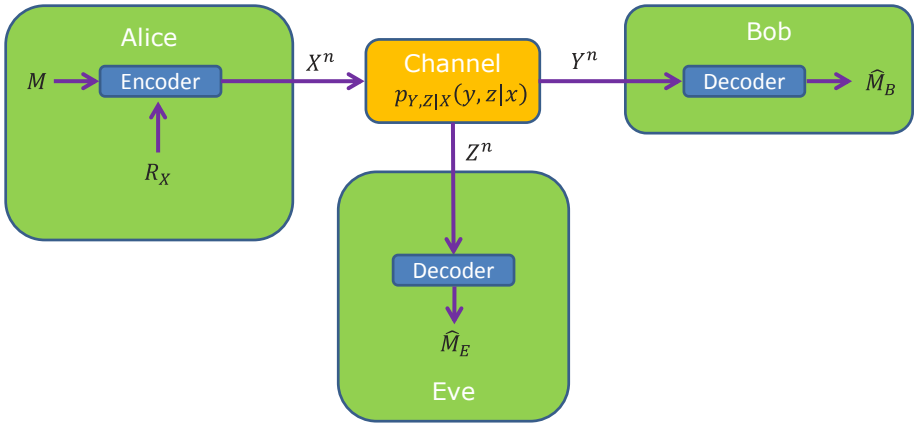


Figure 4: A typical wiretap communication model. M **is the message to be sent,** $\hat{M}_B$ **is Bob's estimated message, and** $\hat{M}_E$ **is Eve's estimated message. The noise property of the channel is quantized by the conditional probability distribution** $p_{Y,Z|X}(y,z|x)$**.** R_X **is produced by Alice's local randomness source.**

where the superscript n denotes the length of the code, and each x_i is a generic element from the signal alphabet $\mathcal{X}$. At the end of the channel, Bob and Eve receive Y^n and Z^n respectively. The security of the channel is measured by the conditional entropy

$$\frac{1}{n}H(M|Z^n). \tag{2.1.14}$$

A rate R for the wiretap channel is achievable with confidential messages if and only if for an arbitrary $\varepsilon > 0$, the following two conditions are satisfied:

$$\begin{aligned} \text{Prob}(\hat{M}_B \neq M) &\leq \varepsilon \\ \frac{1}{n}H(M|Z^n) &\geq R - \varepsilon. \end{aligned} \tag{2.1.15}$$

The *secrecy capacity* of a wiretap channel with confidential messages is defined as the maximal achievable rate R. It is proven [47] that the secrecy capacity of a wiretap channel with confidential messages is given by

$$C_s = \max_{M \to X \to Y,Z} [I(M;Y) - I(M;Z)]. \tag{2.1.16}$$

Eq. 2.1.16 shows that the secrecy capacity of a wiretap channel with confidential

messages coincides with the maximal difference between Alice and Bob's mutual information and Alice and Eve's mutual information.

The wiretap channel enables Alice and Bob transmit secure messages as long as the secrecy capacity is positive. In the wiretap channel, only one-way communication is allowed and there only exists one communication channel. On the other hand, if we allow Alice and Bob to communicate through a public authenticated noiseless channel besides the main noisy channel, they can follow a secret-key agreement procedure and distill secret random key bits even if the secrecy capacity of the main channel is negative. The channel model for secret-key agreement is illustrated in Figure 5. On the two-way public authenticated noiseless channel, Alice and Bob communicate back and forth. By receiving the message B^i produced by Bob on the public authenticated noiseless channel, Alice takes a random variable from her local randomness source, generate a signal symbol x_i and transmit it through a noisy channel characterized by the conditional probability function $p_{Y,Z|X}(y, z|x)$. Alice also generates a message A^i and sends it through the public authenticated noiseless channel to Bob's decoder. Bob receives y_i from the noisy channel and A_i from the public authenticated noiseless channel. He then takes a random number from his local randomness source and produces another message B^{i+1} to be sent on the public channel. B^{i+1} is used by Alice's encoder for the next round. After the communication, Alice and Bob follow a key-distillation procedure in which Alice combines X^n, R_X, A^r, and B^r, and Bob combines Y^n, R_Y, A^r and B^r to produce the key $K \in \mathcal{K} = \{1, 2, ..., 2^{nR}\}$, where R is the secret-key rate.

The secret-key capacity can be obtained by [48]

$$I(X;Y) - \min(I(X,Z), I(Y,Z)) \leq C_s \leq \max(I(X;Y), I(X,Y|Z)), \qquad (2.1.17)$$

where C_s is the maximal achievable secrete-key rate.

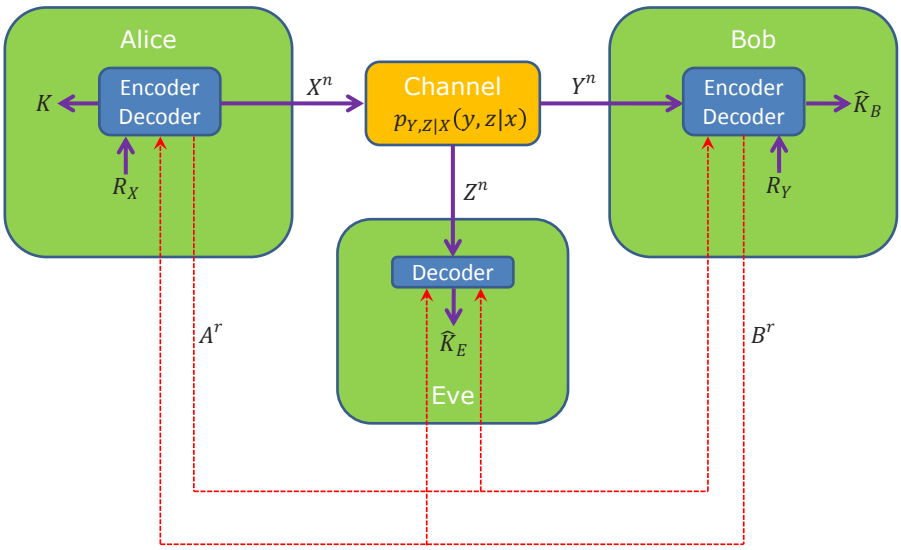


Figure 5: A typical model for secret-key agreement. R_X is produced by Alice's local randomness source. X^n is signal sent by Alice. Y^n is the received signal by Bob. R_Y is produced by Bob's local randomness source. A^r and B^r are generated by their decoders. $\hat{K}_B$ is Bob's estimated key. $\hat{K}_E$ is Eve's estimated key. The noisy channel is characterized by $p_{Y,Z|X}(y,z|x)$. The public authenticated noiseless channel is plotted in dashed red lines.

2.2 Quantum information theory

The classical information theory introduced in Sec. 2.1 deals with the situation where quantum effects are weak enough to be neglected. For a quantum system with prominent quantum effects, the behavior of the system differs from its classical counterpart in the following ways:

- For classical systems, measurements can be infinitely precise. For quantum systems, uncertainty is usually introduced by measurements.

- For classical systems, measurements do not influence the signal being measured. For quantum systems, measurements usually demolish the signal being measured, collapsing the signal state into the measured value.

- For classical systems, an unknown signal can be precisely duplicated. For quantum systems, an arbitrary signal cannot be precisely cloned.

- For classical systems, possible signal states take values from a priorly given set. The signal state can be either element from the set. For quantum systems, possible signal states take values from a priorly given basis set. Unlike the classical situation, the signal state can be a superposition of any elements from the set.

- For classical systems, separated systems are independent. In other words, measurements on one system do not change the states of other systems. For quantum systems, separated systems can be entangled. Measurements on one system can determine the states of other systems.

Taking into account quantum effects, a new theoretical framework is needed to extend classical concepts such as the information unit, the channel capacity, and the secrecy capacity into the quantum world.

2.2.1 Quantum bits

In quantum information theory, the basic unit of quantum information is a quantum bit (qubit), a vector in the Hilbert space. In the Dirac notation, we introduce a basis set $\mathcal{B} = \{|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle\}$, whose elements are eigenvalue-vectors of an *observable* $\hat{O}$:

$$\hat{O}|\psi_i\rangle = \lambda_i|\psi_i\rangle, \tag{2.2.1}$$

where λ_i's are *real* eigenvalues that specify measurement outcomes. These basis vectors possess the following two properties:

$$\begin{aligned} \sum_i |\psi_i\rangle\langle\psi_i| &= I \qquad \text{(Normalizable)} \\ \langle\psi_i|\psi_j\rangle &= \delta_{i,j}, \qquad \text{(Orthogonality)} \end{aligned} \tag{2.2.2}$$

where $\delta_{i,j}$ is the Kronecker symbol, and I is the identity operator. Any vector $|\phi\rangle$ is a superposition of the basis vectors in $\mathcal{B}$:

$$|\phi\rangle = \sum_i \alpha_i |\psi_i\rangle, \tag{2.2.3}$$

where α_i's are complex numbers. In a measurement on $|\phi\rangle$, the probability to obtain outcome λ_i reads $|\alpha_i|^2$. The expected measurement outcome is

$$\langle \hat{O} \rangle = \sum_i |\alpha_i|^2 \lambda_i. \tag{2.2.4}$$

The basis set is not unique. By using another observable $\hat{O}'$ with eigenvalue-vector set $\mathcal{B}' = \{|\psi'_1\rangle, |\psi'_2\rangle, ..., |\psi'_k\rangle\}$, $|\phi\rangle$ can be expanded into a superposition in terms of the eigenvalue-vectors from $\mathcal{B}'$:

$$|\phi\rangle = \sum_i \alpha'_i |\psi'_i\rangle. \tag{2.2.5}$$

Let us introduce a new vector

$$|\phi'\rangle = \sum_i \beta_i |\psi_i\rangle. \tag{2.2.6}$$

The *overlap* between $|\phi\rangle$ and $|\phi'\rangle$ is defined as

$$\langle \phi' | \phi \rangle = \sum_i \alpha_i \beta_i^*, \tag{2.2.7}$$

which is known as the inner product of the two vectors.

Above discussions of qubit assumed that the size of basis set is finite. However, some observables such as the position and the momentum operators possess continuous eigenvalues. Therefore, the size of the corresponding basis set is infinite. In this case, we need to define vectors on a continuous space. The eigenvectors and eigenvalues of a continuous observable $\hat{C}$ satisfy

$$\hat{C}|\psi_\lambda\rangle = \lambda |\psi_\lambda\rangle. \tag{2.2.8}$$

A vector can be expanded into

$$|\phi\rangle = \int f(\lambda)|\psi_\lambda\rangle d\lambda, \tag{2.2.9}$$

where $f(\lambda)$ is the wavefunction to determine the probability density of a measurement on the observable $\hat{C}$. The expected measurement outcome is given by

$$\langle\hat{C}\rangle = \int |f(\lambda)|^2 \lambda d\lambda. \tag{2.2.10}$$

So far, we have introduced qubits used to describe quantum states of *single* systems. As discussed previously, one main difference of quantum systems from classical systems is that several quantum systems can be entangled. To describe entangled quantum systems, one-dimensional qubits are not sufficient. The overall quantum state of two subsystems can be expressed as a two-dimensional quantum state

$$|\Psi^{AB}\rangle = \sum_{i,j} \lambda_{i,j} |\psi_i^A\rangle |\psi_j^B\rangle, \tag{2.2.11}$$

where $|\psi_i^A\rangle$'s belong to the Hilbert space of subsystem A, and $|\psi_j^B\rangle$'s belong to the Hilbert space of the subsystem B. A simple example is the two-photon polarization-entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|0^A\rangle|0^B\rangle + |1^A\rangle|1^B\rangle\right), \tag{2.2.12}$$

where $|0^A\rangle$ and $|0^B\rangle$ denote the horizontal polarization state on the A and B subsystems respectively, and $|1^A\rangle$ and $|1^B\rangle$ denote the vertical polarization state on the A and B subsystems. If a measurement on subsystem A returns $|0^A\rangle$, the state of subsystem B is collapsed into $|0^B\rangle$, and vice versa. One might ask the difference between the quantum entanglement and the classical correlation. To answer this question, we rewrite Eq. 2.2.12 into

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|+^A\rangle|+^B\rangle + |-^A\rangle|-^B\rangle\right), \tag{2.2.13}$$

where

$$|+^j\rangle = \frac{1}{\sqrt{2}}(|0^j\rangle + |1^j\rangle)$$

is the diagonal polarization state and

$$|-^j\rangle = \frac{1}{\sqrt{2}}(|0^j\rangle - |1^j\rangle)$$

is the antidiagonal polarization state, with $j \in \{A, B\}$. Apparently, not only measurements on the horizontal-vertical basis, but also measurements on the diagonal-antidiagonal basis are correlated, which differs from classical correlation because no classical correlation can exist simultaneously on non-commutate basis sets (in this case both the horizontal-vertical basis and the diagonal-antidiagonal basis are correlated). A rigorous treatment of the difference between the quantum entanglement and the classical correlation needs to evaluate the Bell inequality.

2.2.2 von Neumann entropy and Holevo theorem

In classical information theory, a random variable takes values on a set of classical messages with a priorly given probability distribution. For a quantum random variable, it takes values on the set

$$\mathcal{M} = \{|\phi_1\rangle, |\phi_2\rangle, ..., |\phi_n\rangle\},$$

composed of quantum states represented by vectors in the Hilbert space. Similar to classical information theory, the probability distribution of the elements in the set is priorly given. A quantum random variable is defined as the density matrix in the following form:

$$\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|, \tag{2.2.14}$$

where p_i is the probability distribution. Since $|\phi_i\rangle$ can be multi-system states, ρ describes the overall quantum state of an ensemble of quantum systems. In general, any quantum measurement on ρ can be defined as a positive operator valued measure (POVM). A POVM is a set of Hermitian operators that sum to unity:

$$\sum_{i=1}^{n} F_i = I, \tag{2.2.15}$$

where each operator associated with a measurement outcome. If we perform a measurement ρ, the probability the outcome associated with measurement of operator F_i occurs is

$$P(i) = \mathrm{Tr}(\rho F_i). \tag{2.2.16}$$

The density matrix of a subsystem is defined as the reduced density matrix

$$\rho^A \equiv \mathrm{Tr}_B(\rho^{AB}). \tag{2.2.17}$$

Tr_B is a partial trace defined as

$$\mathrm{Tr}_B\left(|\psi_1^A\rangle\langle\psi_2^A| \otimes |\psi_1^B\rangle\langle\psi_2^B|\right) \equiv |\psi_1^A\rangle\langle\psi_2^A|\mathrm{Tr}\left(|\psi_1^B\rangle\langle\psi_2^B|\right), \tag{2.2.18}$$

where $|\psi_1^A\rangle$ and $|\psi_2^A\rangle$ belong to the Hilbert space of subsystem A, and $|\psi_1^B\rangle$ and $|\psi_2^B\rangle$ belong to the Hilbert space of subsystem B.

The analogue to classical entropy is the von Neumann entropy, defined as

$$S(\rho) \equiv -\mathrm{Tr}(\rho \log \rho). \tag{2.2.19}$$

We can also define the quantum conditional entropy, the analogue to the classical conditional entropy, as

$$S(\rho|\sigma) \equiv \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma). \tag{2.2.20}$$

In classical communication, as long as the communication channel is noiseless, Bob's observed signal Y always coincides with Alice's transmitted signal X. Thus, the mutual information between Alice and Bob equals to the entropy of Alice's transmitted signal, i.e., $I(X;Y) = H(X)$. In quantum communication, Alice first encodes classical messages into qubits, which are later transmitted through a quantum channel. On the receiving side, Bob needs to make quantum measurements to estimate Alice's encoded classical messages. This communication model is plotted in Figure 6. Since uncertainty is always introduced by quantum measurements, Bob can no longer

make precise estimate on Alice's encoded classical messages. Suppose Alice has the classical messages set $\mathcal{X} = \{x_1, x_2, ..., x_n\}$ with probability p_i for each message. In the encoding procedure, Alice prepares a quantum state ρ_i, corresponding uniquely to classical message x_i. Once Bob receives the quantum state from the quantum channel, he makes a quantum measurement, resulting in a classical random variable Y. Whatever measurement Bob performs, the mutual information between Alice and Bob is bounded by

$$I(X;Y) \leq S(\rho) - \sum_i p_i S(\rho_i), \tag{2.2.21}$$

where $\rho = \sum_i p_i \rho_i$. Eq. 2.2.21 is known as the Holevo theorem [49], setting an upper bound on the accuracy of Bob's estimate on Alice's messages. The upper bound for $I(X;Y)$ is always referred to as $\chi(X;Y)$.

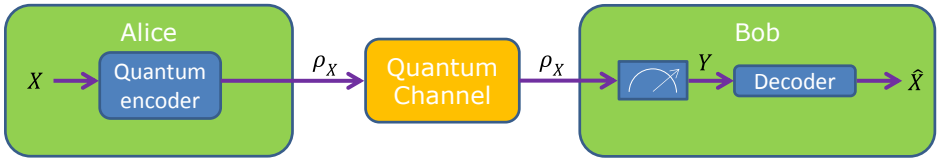


Figure 6: The quantum communication model on a noiseless quantum channel. Alice codes classical message X into qubits ρ_X. Bob performs quantum measurements on ρ_X, and his classical decoding gives estimate $\hat{X}$.

2.2.3 Introduction to quantum key distribution

As one of the applications of quantum communication, quantum key distribution (QKD) [10, 13] is a technique that enables two or more parties, who initially share a secure key, to expand their key with unconditional security. Two fundamental laws in quantum mechanics, i.e., the quantum uncertainty principle and the quantum no-cloning theorem, guarantee the security of QKD. The quantum uncertainty principle sets an ultimate limit on the uncertainty of the outcome from a quantum measurement. According to the quantum uncertainty principle, measurement on a particular physical quantity of a quantum state is always accompany by uncertainty

within a certain range. The measurement uncertainty can be utilized to bound adversary's capability of discriminating quantum messages. In classical communication, transmitted bits can be ideally observed and duplicated. However, in quantum communication, it is impossible to observe precisely an unknown quantum bit (qubit) and to duplicate a new qubit in an identical quantum state, which is known as the quantum no-cloning theorem, denying the possibility to perfectly clone an unknown quantum state. Therefore, an adversary is not able to achieve full information on an unknown qubit. These two fundamental laws in quantum mechanics enable us to design a QKD protocol, allowing us to expand an initially shared key between two or more users with unconditional security. It is shown in Figure 7 a schematic of QKD. QKD follows a typical procedure as follows:

Step 1: State preparation. The sender, usually called Alice, randomly prepares a qubit from a given quantum-state set and sends it through a quantum channel. The quantum channel could be interacted by an adversary, usually called Eve.

Step 2: State measurement. The receiver, usually called Bob, receives the qubit from the quantum channel. Bob then randomly selects a measurement basis from a set of measurement basis. Bob records the classical measurement outcome. Alice and Bob repeat the above two steps until they share classical bits that match the block length of the error-correction code for reconciliation.

Step 3: Channel characterization. Alice and Bob choose a subset of the shared classical bits to estimate physical properties of the quantum channel. According to the quantum uncertainty principle and the quantum no-cloning theorem, either Eve's interference introduces some changes on physical properties of the quantum channel, or Eve's accessible information is bounded to a certain amount.

Step 4: Reconciliation. If the physical properties of the quantum channel are in a secure region, i.e., positive secret-key capacity exists, Alice and Bob follow a reconciliation protocol on a public authenticated noiseless classical channel to agree

on a string $s^n = \{s_1, s_2, ..., s_n\}$. Each element of the vector is a random variable following the same probability distribution as the random variable S does. Everyone can read information on the classical channel, but the transmitted message cannot be modified. Alice and Bob's initial shared key serves as the message-authentication key.

We need to note here that there exist two kinds of reconciliation protocols. For a forward reconciliation based protocol, Bob tries to recover the classical information that Alice sent by means of quantum signals. In this case, Alice needs to generate some redundant messages that serve as checkbits and send them through a public authenticated noiseless classical channel. Let Alice the encoded random variable be a vector $x^n = \{x_1, x_2, ..., x_n\}$. Each element of the vector is a random variable following the same probability distribution as the random variable X does. Bob's received classical information is a vector $y^n = \{y_1, y_2, ..., y_n\}$. Each element of the vector is a random variable following the same probability distribution as the random variable Y does. the checkbits are generated by a function $m^k = G(x^n)$. Once Bob receives the checkbits, he performs a decoding operation to correct all errors introduced by additional channel noise or quantum noise from his measurements. His decoding operation can be described by $s^n = D(y^n, m^k) = F(x^n)$, where F is a transformation function by Alice. The efficiency of reconciliation is given by

$$\beta = \frac{H(S)}{I(X;Y)}. \tag{2.2.22}$$

for large n.

However, continuous-variable QKD protocols based on forward reconciliation do not tolerate more than 50% of channel loss because if we give the lost signal to Eve, she always have a better view of Alice's original data than Bob does. To overcome this problem, reverse reconciliation must be introduced into QKD protocols. For a reverse reconciliation based protocol, Alice tries to recover the classical information obtained by Bob. In this case, Bob needs to generate some redundant messages that serve as

checkbits and send them through a public authenticated noiseless classical channel. Once Alice receives the checkbits, he performs a decoding operation trying to agree on a string s^n with Bob. Since Alice always have a better view on Bob's received signal than Eve does, reverse reconciliation can in principle extend the communication distance to infinity if the quantum channel is noiseless.

The complexity of reconciliation depends on the error-correction code that Alice and Bob use. The complexity of reconciliation on binary bits is usually much lower than reconciliation on continuous variables.

Step 5: Privacy amplification. In this stage, Alice and Bob share a string s^n. To remove Eve's information on s^n, Alice and Bob need to a function that maps the input string $s^n \in \mathcal{S}$ into the output set $k^l \in \mathcal{K}$. If we carefully design the function, Eve will not have any information on k^l. Universal hash functions satisfy our need. A universal hash function family $\mathcal{H}$ satisfies $\forall s_1^n, s_2^n \in \mathcal{S}, s_1^n \neq s_2^n, \forall h \in \mathcal{H}$: $\Pr\left[h(s_1^n) = h(s_2^n)\right] \leq \frac{1}{|\mathcal{K}|}$. k^l serves as the final secure key between Alice and Bob.

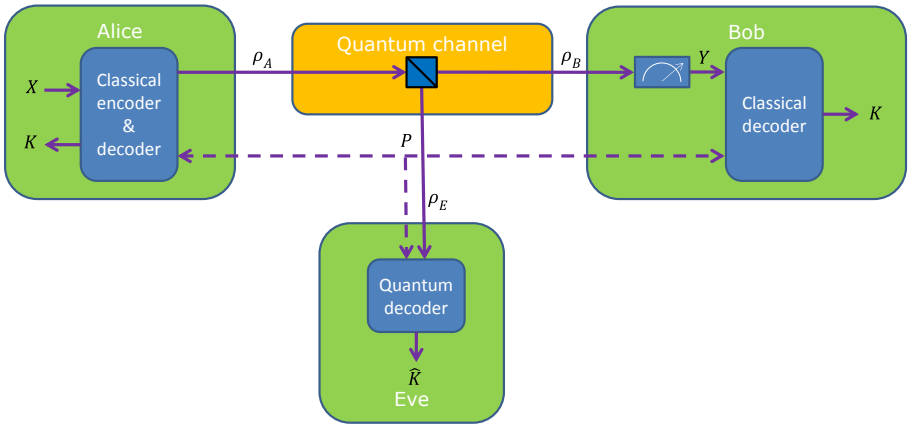


Figure 7: A schematic of quantum key distribution. Alice converts the classical random message X into qubits represented by ρ_A. The qubits received by Bob and Eve are ρ_B and ρ_E respectively. Bob's quantum measurements lead to classical random variable Y for decoding. Based on Y, P is produced as the reconciliation message on a public authenticated noiseless classical channel. Based on the qubits ρ_E and P, the quantum decoding of Eve yields $\hat{K}$ as the estimate of the final key K.

Many results discuss the security of QKD systems. For the state of the art, the unconditional security for discrete-variable QKD systems against the most general attacks has been proven [50]. For continuous-variable QKD systems with both Gaussian and discrete modulation, the security against collective attacks, where Eve makes individual interactions but overall measurements, is proven in [51–57]. Quantum de Finetti theorem for infinite dimensional Hilbert space is proven in [58], which implies that continuous-variable QKD protocols that are secure against collective attacks are asymptotically secure against coherent attacks, which are the most general kind of attacks.

2.3 Quantum optics

The topics discussed in Sec. 2.2 are mathematically abstract. In reality, quantum information needs to be stored in physical carriers, such as electrons, atoms, and photons. In this section, we will focus on the physics of photon by introducing its physical origin, its quantum description, and measurements on it.

2.3.1 Quantization of electromagnetic field

The dynamics of electromagnetic field in free space is governed by the Maxwell equations:

$$\nabla \cdot \mathbf{E} = \frac{\rho}{\varepsilon_0} \qquad \text{(Gauss' law)} \tag{2.3.1a}$$

$$\nabla \cdot \mathbf{B} = 0 \qquad \text{(Gauss' law for magnetism)} \tag{2.3.1b}$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \qquad \text{(Faraday' law of induction)} \tag{2.3.1c}$$

$$\nabla \times \mathbf{B} = \mu_0 \mathbf{J} + \mu_0 \varepsilon_0 \frac{\partial \mathbf{E}}{\partial t} \qquad \text{(Ampère's circuital law).} \tag{2.3.1d}$$

We next introduce the vector potential

$$\mathbf{B} = \nabla \times \mathbf{A}, \tag{2.3.2}$$

and the scalar potential

$$\nabla\phi = -\mathbf{E} - \frac{\partial \mathbf{A}}{\partial t}. \tag{2.3.3}$$

By inserting Eq. 2.3.2 and Eq. 2.3.3 into the Maxwell equations in Eqs. 2.3.1, we arrive at the following differential equations for $\mathbf{A}$ and ϕ:

$$\nabla^2\mathbf{A} - \mu_0\varepsilon_0\frac{\partial^2\mathbf{A}}{\partial t^2} = -\mu_0\mathbf{J} + \nabla\left(\nabla\cdot\mathbf{A} + \mu_0\varepsilon_0\frac{\partial\phi}{\partial t}\right) \tag{2.3.4a}$$

$$\nabla^2\phi + \frac{\partial}{\partial t}\left(\nabla\cdot\mathbf{A}\right) = -\frac{\rho}{\varepsilon_0}. \tag{2.3.4b}$$

There does not exist an unique choice for either $\mathbf{A}$ or ϕ. To see this, we make a transform

$$\mathbf{A} = \mathbf{A}' - \nabla\Xi, \tag{2.3.5}$$

and

$$\phi = \phi' + \frac{\partial\Xi}{\partial t}, \tag{2.3.6}$$

where Ξ is an arbitrary function in space and time. Inserting Eq. 2.3.5 and Eq. 2.3.6 into the definition of $\mathbf{A}$ in Eq. 2.3.2 and the definition of ϕ in Eq. 2.3.3, we find that $\mathbf{E}$ is unchanged by the transform. One commonly used choice of the vector potential

$$\nabla\cdot\mathbf{A} = 0, \tag{2.3.7}$$

which is known as the Coulomb gauge. In the Coulomb gauge and in free space, Eq. 2.3.4a becomes

$$-\nabla^2\mathbf{A} + \frac{1}{c^2}\frac{\partial^2\mathbf{A}}{\partial t^2} = 0. \tag{2.3.8}$$

As a trial solution to Eq. 2.3.8, $\mathbf{A}$ is expanded as a superposition of wavevector modes:

$$\begin{aligned}\mathbf{A}(\mathbf{r},t) &= \sum_{\mathbf{k}} A_{\mathbf{k}}(\mathbf{r},t) + \text{c.c.} \\ &= \sum_{\mathbf{k}} A_{\mathbf{k}}(t)e^{i\mathbf{k}\cdot\mathbf{r}} + \text{c.c.},\end{aligned} \tag{2.3.9}$$

where the time-dependent part $\mathbf{A}_\mathbf{k}(t)$ and the spatial-dependent part $e^{i\mathbf{k}\cdot\mathbf{r}}$ are separated, and c.c is the complex conjugate. Plugging Eq. 2.3.9 into Eq.2.3.8 and separating different wavevector modes yield the differential equation for the time-varying part of each wavevector mode:

$$\frac{\partial^2 \mathbf{A}_\mathbf{k}(t)}{\partial t^2} + \omega^2 \mathbf{A}_\mathbf{k}(t) = 0, \tag{2.3.10}$$

with the plane-wave solution

$$\mathbf{A}_\mathbf{k}(\mathbf{r}, t) = \mathbf{A}_\mathbf{k} e^{-\omega t + i\mathbf{k}\cdot\mathbf{r}} + \text{c.c.} \tag{2.3.11}$$

In a cubic space with volume $V = L^3$, the time-averaged energy of the field reads

$$E_\mathbf{k} = \frac{1}{2T} \int_0^T dt \int_V \left(\varepsilon_0 \mathbf{E}_\mathbf{k}^2 + \frac{1}{\mu_0} \mathbf{B}_\mathbf{k}^2 \right) d\mathbf{r}^3, \tag{2.3.12}$$

where T is the period of oscillation. Inserting the vector potential definition in Eq. 2.3.2, the scalar potential definition in Eq. 2.3.3, and the Coulomb gauge condition in Eq. 2.3.7 into Eq. 2.3.12, it yields

$$E_\mathbf{k} = 2\varepsilon_0 V \omega^2 |\mathbf{A}_\mathbf{k}|^2. \tag{2.3.13}$$

Let

$$\mathbf{A}_\mathbf{k} = \frac{1}{\sqrt{4\varepsilon_0 V m\omega^2}} \left(m\omega q + ip \right) \hat{\mathbf{n}}_\mathbf{k}, \tag{2.3.14}$$

where $\hat{\mathbf{n}}_\mathbf{k}$ is a unit vector on $\mathbf{k}$. The electromagnetic field oscillation is analogue to a classical harmonic oscillator with classical energy

$$H = \frac{1}{2} \left(\frac{p^2}{m} + m\omega^2 q^2 \right), \tag{2.3.15}$$

where p is the canonic momentum, and q is the canonic position. The quantum-mechanical Hamiltonian of a harmonic oscillator can be derived by replacing the classical canonic momentum and position with *quantum operators*:

$$\hat{H} = \frac{1}{2} \left(\frac{\hat{p}^2}{m} + m\omega^2 \hat{q}^2 \right). \tag{2.3.16}$$

$\hat{p}$ and $\hat{q}$ satisfy the commutation relation $[\hat{q}, \hat{p}] = \hat{q}\hat{p} - \hat{p}\hat{q} = i\hbar$. We next define the *annihilation* and the *creation* operators as

$$\hat{a} = \sqrt{\frac{m\omega}{2\hbar}}\hat{q} + \frac{i}{\sqrt{2\hbar m\omega}}\hat{p} \tag{2.3.17a}$$

$$\hat{a}^\dagger = \sqrt{\frac{m\omega}{2\hbar}}\hat{q} - \frac{i}{\sqrt{2\hbar m\omega}}\hat{p} \tag{2.3.17b}$$

with

$$\left[\hat{a}, \hat{a}^\dagger\right] = 1 \tag{2.3.18}$$

satisfied. The Hamiltonian is reorganized into

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) = \hbar\omega\left(\hat{n} + \frac{1}{2}\right), \tag{2.3.19}$$

where

$$\hat{n} \equiv \hat{a}^\dagger\hat{a} \tag{2.3.20}$$

is referred to as the *number operator*. Let $|n\rangle$ be the energy eigenstate of the Hamiltonian $\hat{H}$ with the eigenvalue E_n. By making use of the commutation relation in Eq. 2.3.18, we find [59]

$$\hat{H}|n\rangle = \left(n + \frac{1}{2}\right)\hbar\omega|n\rangle. \tag{2.3.21}$$

Applying the annihilation and the creation operators on $|n\rangle$ yields

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \tag{2.3.22}$$

and

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \tag{2.3.23}$$

respectively.

2.3.2 Fock state and coherent state

The energy eigenstates $\hat{H}$ are named the number states or the *Fock states*. The Fock state $|0\rangle$ is the vacuum state, corresponding the ground state of a harmonic oscillator. It is interesting to see that the eigenvalue of the vacuum state is $\frac{1}{2}\hbar\omega$. Consequently,

the background energy of vacuum is nonzero. The state $|n\rangle$ is related to the vacuum state $|0\rangle$ by

$$|n\rangle = \frac{1}{\sqrt{n!}} \left(\hat{a}^\dagger\right)^n |0\rangle. \tag{2.3.24}$$

We next introduce a state

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{2.3.25}$$

where α is a complex number. Applying the annihilation operator on $|\alpha\rangle$ yields

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle, \tag{2.3.26}$$

showing that $|\alpha\rangle$ is an eigenstate of $\hat{a}$. The eigenstates of the annihilation operator $\hat{a}$ are defined as the *coherent states*. Since $\hat{a}$ is not a Hermitian operator whose eigenvalues are real, its eigenvalues are not measurable. The probability of finding n photons in $|\alpha\rangle$ reads

$$|\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!}, \tag{2.3.27}$$

following a *Poisson distribution*. We next introduce two *quadrature operators*

$$\hat{X} = \frac{1}{2} \left(\hat{a} + \hat{a}^\dagger\right) \tag{2.3.28a}$$

$$\hat{Y} = \frac{1}{2i} \left(\hat{a} - \hat{a}^\dagger\right). \tag{2.3.28b}$$

$\hat{X}$ and $\hat{Y}$ satisfy the commutation relation

$$[\hat{X}, \hat{Y}] = \frac{i}{2}. \tag{2.3.29}$$

The Hamiltonian can be expressed in terms of the quadrature operators:

$$\hat{H} = \hbar\omega \left(\hat{X}^2 + \hat{Y}^2\right). \tag{2.3.30}$$

For the coherent state $|\alpha\rangle$, the expected values of the two quadrature operators are

$$\begin{aligned} \overline{X} &= \langle\alpha|\hat{X}|\alpha\rangle = \frac{1}{2}\left(\alpha + \alpha^*\right) = \Re(\alpha) \\ \overline{Y} &= \langle\alpha|\hat{Y}|\alpha\rangle = \frac{1}{2i}\left(\alpha - \alpha^*\right) = \Im(\alpha), \end{aligned} \tag{2.3.31}$$

and the expected variances of the two quadrature operators are

$$\begin{aligned} \Delta X^2 &\equiv \overline{X^2} - \overline{X}^2 = \frac{1}{4} \\ \Delta Y^2 &\equiv \overline{Y^2} - \overline{Y}^2 = \frac{1}{4}. \end{aligned} \tag{2.3.32}$$

The Heisenberg uncertainty principle

$$\Delta X \Delta Y \geq \frac{1}{4} \tag{2.3.33}$$

holds for any coherent state. Thus, coherent states are a minimal uncertainty states.

We now discuss the quantum dynamics of coherent state. In the Heisenberg picture, the time evolution of the creation and annihilation operators can be obtained by solving the time dependent equations

$$\frac{d\hat{a}}{dt} = \frac{i}{\hbar}\left[\hat{H}, \hat{a}\right] \tag{2.3.34a}$$

$$\frac{d\hat{a}^\dagger}{dt} = \frac{i}{\hbar}\left[\hat{H}, \hat{a}^\dagger\right], \tag{2.3.34b}$$

giving solutions

$$\hat{a}(t) = \hat{a}(0)e^{-i\omega t} \tag{2.3.35a}$$

$$\hat{a}^\dagger(t) = \hat{a}^\dagger(0)e^{i\omega t}. \tag{2.3.35b}$$

The time evolution of the expected values of $\hat{X}$ and $\hat{Y}$ is

$$\overline{X}(t) = \langle\alpha|\hat{X}(t)|\alpha\rangle = \overline{X}(0)\cos(\omega t) \tag{2.3.36a}$$

$$\overline{Y}(t) = \langle\alpha|\hat{Y}(t)|\alpha\rangle = \overline{Y}(0)\sin(\omega t). \tag{2.3.36b}$$

Therefore, the quantum dynamics of coherent states resemble the oscillating behavior of electromagnetic field. In fact, the output from a laser can be approximately described by a coherent state, regarded as the closest quantum state to classical physics.

2.3.3 Quantum measurements

So far, we have briefly introduced the quantization of electromagnetic field and the most common quantum states arising from the quantization. We will next introduce quantum measurements on the quantum states. We have introduced two important physical quantities: the photon number and the field quadratures. To make measurements on the photon number of a field, a light beam containing the field is sent to a photon detector. There exist two kinds of photon detectors. PiN diodes with high bandwidth (from GHz to THz) are the most commonly used photon detectors for telecommunication. Classically, PiN diodes measure the intensity of the incoming field. Ideally, a PiN diode with perfect detection efficient and unlimited bandwidth converts every incident photon into an electron in the produced photocurrent. Therefore, the amplitude of the photocurrent is proportional to the time derivative of the photon number. Quantum mechanically, the relation between the operators is

$$\hat{i}(t) \propto \frac{d\hat{N}(t)}{dt}. \tag{2.3.37}$$

In practice, both the signal and the detector are bandwidth limited. To capture all information contained in the signal, the bandwidth of the detector needs to be higher than the bandwidth of the signal to make a single-mode measurement. A filter is usually installed at the output of PiN diode to get rid of additional out-of-band noise. A detection schematic of a quantum measurement using PiN diode is shown in Figure 8.

Although PiN diodes possess high detection bandwidth, they are not able to perform measurements on weak signals at the single-photon level because the photocurrent is contaminated by dark current and electronic noise. To detect extremely weak signals at the single-photon level, avalanche photodiodes (APD) are used. The quantum efficiency of APD is wavelength dependent. The highest quantum efficiency

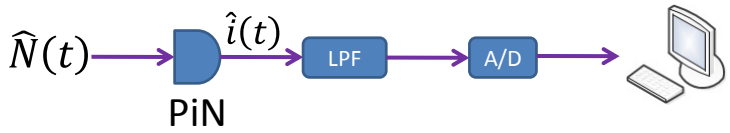


Figure 8: A schematic of a quantum measurement using PiN detectors. LPF is a low-pass filter to get rid of out-of-band noise. A/D is an analog-to-digital converter to produce digital signal that is processed later.

around 80% is achieved at visible wavelengths. To perform photon counting on optical pulses, synchronization circuits are usually needed to reduce detector noise and increase quantum efficiency. A detection schematic of APD is drawn in Figure 9.

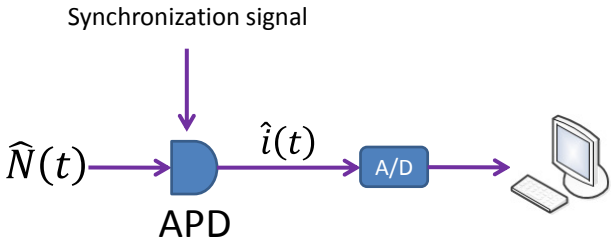


Figure 9: A schematic of photon detection using APD detectors.

To obtain information of field quadratures, homodyne measurement is utilized. To perform a homodyne measurement, a strong local oscillator (LO) is mixed with a signal beam by a beam splitter (BS). The output from the BS is injected into a PiN diode. A schematic of homodyne measurement is shown in Figure 10. Let the electric field operator for the LO be $\hat{E}_{LO}$ and the electric field operator of the signal be $\hat{E}_S$, the produced photocurrent is related to the two field operators by

$$\begin{aligned} \hat{i}(t) &\propto |\sqrt{R}\hat{E}_{LO}e^{-i\theta} + \sqrt{1-R}\hat{E}_S|^2 \\ &= R|E_{LO}|^2 + \sqrt{R(1-R)}E_{LO}\left(\hat{E}_S e^{-i\theta} + \hat{E}_S e^{i\theta}\right), \end{aligned} \tag{2.3.38}$$

where R is the transmissivity of the BS. In the second line of Eq. 2.3.38, we replaced

$\hat{E}_{LO}$ by a complex field amplitude based on the fact that the LO intensity is much stronger than the signal intensity. By use of a strong LO, homodyne measurement can detect quadrature information of very weak fields at the single-photon level and achieve high contrast against dark current, which is usually 10 dB below the signal photocurrent. By varying the phase of the LO, any quadrature of the signal can be measured.

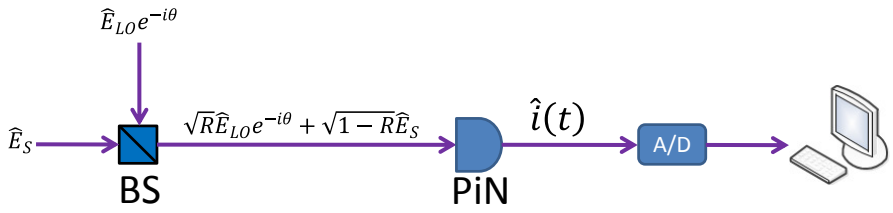


Figure 10: Aschematic of homodyne measurement.

However, the homodyne measurement schematic shown in Figure 10 suffers from the side-band excess noise of the LO. To overcome this problem, balanced homodyne measurement shown in Figure 11 needs to be used. In a balanced detection scheme, excess noise from the side-band of the LO is canceled by a subtraction of the two photocurrents produced by the two different PiN diodes at the two outputs of a 50/50 BS. The difference photocurrent reads

$$\hat{i}(t) \propto E_{LO}\left(\hat{E}_S e^{-i\theta} + \hat{E}_S e^{i\theta}\right). \tag{2.3.39}$$

The photocurrent is then fed to a bandpass filter to erase excess out-of-band noise. The filtered signal is amplified by an electronic amplifier and finally frequency transformed into the baseband by a mixer. The baseband signal is sampled by acquisition electronics.

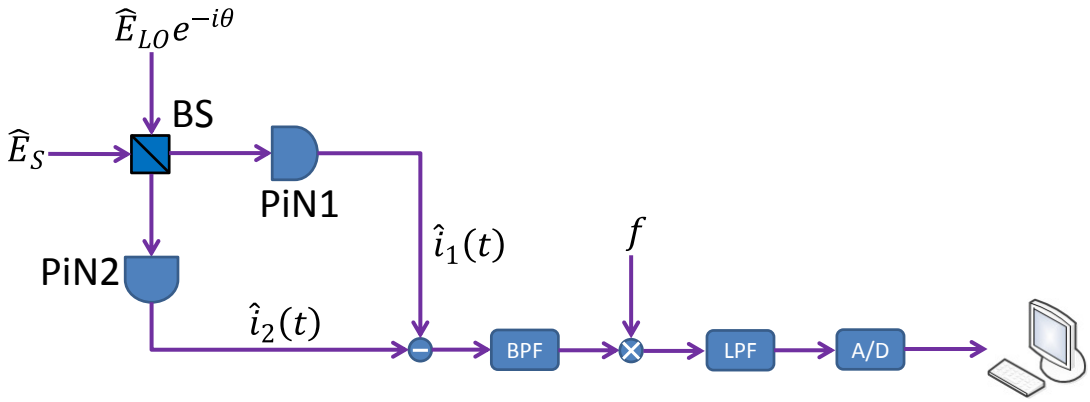


Figure 11: Aschematic of balanced homodyne measurement.

2.4 Nonlinear optics

In Sec. 2.3, basics of quantum optics is introduced. We have discussed two important quantum states of the quantized electromagnetic field, i.e., the Fock state and the coherent state. The coherent state is the quantum state that possesses the closest behavior to classical physics. In fact, the Fock state and other quantum states such as the squeezed state and the entangled state behave nonclassically and can lead to various applications in quantum communications. In quantum key distribution, Fock states containing only one photon per pulse are desired to guarantee the security of key generation. The entangled states are not only applied in entanglement-based quantum key distribution protocols, but are also necessary for quantum teleportation and quantum dense encoding. However, unlike the coherent state that can be generated directly from lasers, generation of nonclassical quantum states usually require nonlinear optical processes. In this section, preliminaries of nonlinear optics will be covered. In the first part of this section, nonlinear susceptibilities, which are used to quantify the nonlinearity of materials, will be defined. In the second part, we will focus on light-matter interaction, from which nonlinearities are originated.

2.4.1 Nonlinear susceptibility

When an electromagnetic wave is propagating in matter, the macroscopic Maxwell equations are used to describe its dynamics:

$$\nabla \cdot \mathbf{D} = \rho_f \tag{2.4.1a}$$

$$\nabla \cdot \mathbf{B} = 0 \tag{2.4.1b}$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \tag{2.4.1c}$$

$$\nabla \times \mathbf{H} = \mathbf{J}_f + \frac{\partial \mathbf{D}}{\partial t}, \tag{2.4.1d}$$

where ρ_f is the free charge and $\mathbf{J}_f$ is the free current density. The constitutive relations, which relate the propagating wave with the response of the matter, are

$$\mathbf{D} = \varepsilon_0 \mathbf{E} + \mathbf{P} \tag{2.4.2a}$$

$$\mathbf{H} = \frac{1}{\mu_0}\mathbf{B} - \mathbf{M}, \tag{2.4.2b}$$

where $\mathbf{P}$ is the polarization field. $\mathbf{P}$ can be expanded to arbitrary orders of the electric field:

$$\begin{aligned} \mathbf{P} &= \mathbf{P}^{(1)} + \mathbf{P}^{(2)} + \mathbf{P}^{(3)} + \cdots \\ &= \varepsilon_0 \left(\chi^{(1)} \cdot \mathbf{E} + \chi^{(2)} : \mathbf{EE} + \chi^{(3)} \vdots \mathbf{EEE} + \cdots \right). \end{aligned} \tag{2.4.3}$$

In the time domain, the polarization field to each order can be expressed as

$$\mathbf{P}^{(1)}(\mathbf{r}, t) = \varepsilon_0 \int_{-\infty}^{\infty} \chi^{(1)}(t-\tau) \cdot \mathbf{E}(\mathbf{r}, \tau) d\tau \tag{2.4.4a}$$

$$\mathbf{P}^{(2)}(\mathbf{r}, t) = \varepsilon_0 \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \chi^{(2)}(t-\tau_1, t-\tau_2) : \mathbf{E}(\mathbf{r}, \tau_1)\mathbf{E}(\mathbf{r}, \tau_2) d\tau_1 d\tau_2 \tag{2.4.4b}$$

$$\mathbf{P}^{(3)}(\mathbf{r}, t) = \varepsilon_0 \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \chi^{(3)}(t-\tau_1, t-\tau_2, t-\tau_3) \vdots \mathbf{E}(\mathbf{r}, \tau_1)\mathbf{E}(\mathbf{r}, \tau_2)\mathbf{E}(\mathbf{r}, \tau_3) d\tau_1 d\tau_2 d\tau_3 \tag{2.4.4c}$$

The wave propagation dynamics can be obtained by solving the propagation equation written in terms of $\mathbf{E}$ and $\mathbf{P}$:

$$\nabla^2 \mathbf{E} + \frac{1}{c^2}\frac{\partial^2 \mathbf{E}}{\partial t^2} = -\mu_0 \frac{\partial^2 \mathbf{P}}{\partial t^2}. \tag{2.4.5}$$

We note here that only materials that are inversion asymmetric possess the $\chi^{(2)}$ nonlinearity. For central symmetric material such as silica and graphene, the lowest-order nonlinear susceptibility is $\chi^{(3)}$.

2.4.2 Light-matter interaction

The Hamiltonian of an electron in an atom is

$$H_0 = \frac{\mathbf{p}^2}{2m} + V(\mathbf{r}), \tag{2.4.6}$$

where $\mathbf{p}$ is the momentum operator, and $\mathbf{r}$ is the position operator. When the electron is coupled to an external electromagnetic field, the overall Hamiltonian can be obtained by a minimal substitution $\mathbf{p} \to \mathbf{p} + e\mathbf{A}(t)$:

$$H = \frac{\left[\mathbf{p} + e\mathbf{A}(t)\right]^2}{2m} + V(\mathbf{r}), \tag{2.4.7}$$

where $\mathbf{A}(t)$ is the vector potential defined in Eq. 2.3.2. We choose the Coulomb gauge so that $\nabla \cdot \mathbf{A} = 0$. Eq. 2.4.7 can be expanded as

$$H = H_0 + \frac{e}{2m}\left[\mathbf{p} \cdot \mathbf{A}(t) + \mathbf{A}(t) \cdot \mathbf{p}\right], \tag{2.4.8}$$

where the second-order term $|\mathbf{A}(t)|^2$ is dropped under the assumption that field intensity is relatively weak. The Hamiltonian H can be expressed as the sum of the free-electron Hamiltonian H_0 and a time-varying contribution

$$V(t) = \frac{e}{2m}\left[\mathbf{p} \cdot \mathbf{A}(t) + \mathbf{A}(t) \cdot \mathbf{p}\right]. \tag{2.4.9}$$

Since $\mathbf{p} = -i\hbar\nabla$ and $\nabla \cdot \mathbf{A} = (\nabla \cdot \mathbf{A}) + \mathbf{A} \cdot \nabla$, in the Coulomb gauge we end up with $\mathbf{p} \cdot \mathbf{A}(t) = \mathbf{A}(t) \cdot \mathbf{p}$. $V(t)$ then becomes

$$V(t) = \frac{e}{m}\mathbf{A}(t) \cdot \mathbf{p}. \tag{2.4.10}$$

In the Coulomb gauge, the vector potential of a plane wave can be written as

$$\mathbf{A}(t) = Ae^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)}\hat{\mathbf{n}} + \text{c.c.}, \tag{2.4.11}$$

where $\hat{\mathbf{n}}$ is a unit vector on the polarization of the wave. If the interaction length is much shorter than the size of a molecule, we have $e^{i\mathbf{k}\cdot\mathbf{r}} \approx 1$, known as the electric-dipole approximation. Under the electric-dipole approximation, $V(t)$ reads

$$V(t) = \frac{e}{m}\left[Ae^{-i\omega t}\hat{\mathbf{n}}\cdot\mathbf{p} + \text{c.c.}\right], \tag{2.4.12}$$

where c.c. denotes the complex conjugate. Now let us consider the average transition rate from the state $|i\rangle$ to $|f\rangle$. For $V(t) = V_0 e^{-i\omega t}$, the average transition rate can be calculated with [59]

$$R_{i\to f} = \frac{2\pi}{\hbar}|\langle f|V_0|i\rangle|^2\delta\left(E_f - E_i - \hbar\omega\right). \tag{2.4.13}$$

Substituting Eq. 2.4.12 into Eq. 2.4.13 yields

$$R_{i\to f} = \frac{2\pi e^2 A^2}{m^2\hbar}|\langle f|\hat{\mathbf{n}}\cdot\mathbf{p}|i\rangle|^2\left[\delta\left(E_f - E_i - \hbar\omega\right) + \delta\left(E_f - E_i + \hbar\omega\right)\right]. \tag{2.4.14}$$

If the energy dispersion is parabolic, i.e., the dependence of H_0 and $\mathbf{p}$ is quadratic, the equality

$$\mathbf{p} = -\frac{im}{\hbar}\left[\mathbf{r}, H_0\right] \tag{2.4.15}$$

holds. By replacing $\mathbf{p}$ with Eq. 2.4.15, the average transition probability can be rewritten as

$$\begin{aligned} R_{i\to f} &= \frac{2\pi e^2 A^2\omega_{fi}^2}{\hbar^2}|\langle f|\hat{\mathbf{n}}\cdot\mathbf{r}|i\rangle|^2\left[\delta(\omega_{fi}-\omega) + \delta(\omega_{fi}+\omega)\right] \\ &= \frac{2\pi e^2 E^2}{\hbar^2}|\langle f|\hat{\mathbf{n}}\cdot\mathbf{r}|i\rangle|^2\left[\delta(\omega_{fi}-\omega) + \delta(\omega_{fi}+\omega)\right], \end{aligned} \tag{2.4.16}$$

where $\omega_{fi} = (E_f - E_i)/\hbar$, and the relation $E = \omega A$ has been used. Define the dipole operator as

$$\boldsymbol{\mu} = -e\mathbf{r}, \tag{2.4.17}$$

and the dipole-interaction (or called direct coupling) Hamiltonian

$$V'(t) = -\boldsymbol{\mu}\cdot\mathbf{E}(t). \tag{2.4.18}$$

By calculating the new average transition rate $R'_{i\to f}$, we find that $R'_{i\to f} = R_{i\to f}$. This argument shows that the time-varying Hamiltonians $V(t)$ and $V'(t)$ lead to identical quantum dynamics as long as the energy dispersion of the electron is parabolic. In other words, for non-relativistic electrons, the two different Hamiltonians are equivalent.

Let the Hamiltonian be

$$H = H_0 - \boldsymbol{\mu} \cdot \mathbf{E}(t) = H_0 + V(t), \tag{2.4.19}$$

and the eigenstates of H_0 be $\{|1\rangle, |2\rangle, ..., |m\rangle, ..., |n\rangle, ...\}$. The eigenstate equation is

$$H_0|m\rangle = E_m|m\rangle. \tag{2.4.20}$$

The quantum dynamics of an electron can be obtained by solving the time-dependent Schrödinger equation in the energy-eigenstate representation within the density-matrix formalism [60]:

$$\dot{\rho}_{mn} = -\frac{i}{\hbar}\left[H, \rho\right]_{mn}, \tag{2.4.21}$$

where ρ is the density matrix of the electron and $A_{mn} = \langle m|A|n\rangle$. Eq. 2.4.21 does not take into account relaxation processes cause by electron-electron scattering and electron-phonon scattering. A complete treatment of such relaxation processes requires sophisticated quantum-mechanical calculations [61]. For the simplest model, such relaxation processes can be modelled by introducing phenomenological decay constants into Eq. 2.4.21, yielding

$$\dot{\rho}_{mn} = -\frac{i}{\hbar}\left[H, \rho\right] - \Gamma_{mn}\left(\rho_{mn} - \rho^{eq}_{mn}\right), \tag{2.4.22}$$

where Γ_{mn} is the decay constant, and ρ^{eq}_{mn} is the value of ρ_{mn} in thermal equilibrium.

Eq. 2.4.22 can not be solved analytically in general. Two methods are usually utilized to solve Eq. 2.4.22. *The perturbative method* can be used when the population inversion is small. It is usually applicable for non-resonant interactions where the light

frequency is not close to any of the resonant frequencies of the atom. When the light frequency is close to the resonant frequency of the atom and large population inversion is induced, the *nonperturbative method* needs to be used.

For the perturbative method, it is assumed that the density matrix can be expanded as the sum of density matrices with different orders:

$$\rho = \rho^{(0)} + \rho^{(1)} + \rho^{(2)} + \cdots , \tag{2.4.23}$$

Each order is cascadedly solved by

$$\dot{\rho}^{(0)}_{mn} = -i\omega_{mn}\rho^{(0)}_{mn} - \Gamma_{mn}\left(\rho^{(0)}_{mn} - \rho^{(0)}_{eq}\right) \tag{2.4.24a}$$

$$\dot{\rho}^{(1)}_{mn} = -(i\omega_{mn} + \Gamma_{mn})\rho^{(1)}_{mn} - \frac{i}{\hbar}[V(t), \rho^{(0)}]_{mn} \tag{2.4.24b}$$

$$\dot{\rho}^{(2)}_{mn} = -(i\omega_{mn} + \Gamma_{mn})\rho^{(2)}_{mn} - \frac{i}{\hbar}[V(t), \rho^{(1)}]_{mn}. \tag{2.4.24c}$$

The polarization field is obtained by evaluating the expected value of the induced dipole moment:

$$\mathbf{P} = N\langle \boldsymbol{\mu}(t)\rangle = N\mathrm{Tr}\left[\rho(t)\boldsymbol{\mu}\right], \tag{2.4.25}$$

where N is the density of atoms. knowing the polarization field $\mathbf{P}$, Eq. 2.4.3 can be used to separate different frequency-dependent nonlinear susceptibilities $\chi^{(i)}(\omega)$.

When the frequency of the strong laser is resonant with the atom, many electrons are pumped from the ground state to the excited state. In this case, the perturbative method, which assumes that the population inversion is small, is not valid. We next introduce the non-perturbative method, based on which the resonant nonlinearity can be examined.

Let us consider the two-level model for semiconductors. In the two-level model, only two energy eigenstates exist, i.e., the valance-band state $|V\rangle$ and the conduction-band state $|C\rangle$. The quantum dynamics is governed by [60]

$$\dot{\rho}_{CV} = -(\omega_{VC} + \Gamma_2)\rho_{VC} + \frac{i}{\hbar}V_{VC}\varrho \tag{2.4.26a}$$

$$\dot{\varrho} = -\Gamma_1(\varrho - \varrho^{eq}) - \frac{2i}{\hbar}(V_{CV}\rho_{VC} - V_{VC}\rho_{CV}), \tag{2.4.26b}$$

where $\varrho = \rho_{VV} - \rho_{CC}$. Γ_1 is the population-relaxation decay rate, and Γ_2 is the decoherence rate. The general form for the interacting-matrix element V_{VC} is

$$V_{VC} = -\mu_{VC}\left(Ee^{-i\omega t} + E^* e^{i\omega t}\right). \tag{2.4.27}$$

By assuming that the scattering rates are much less than the resonant frequency, i.e., $\omega_{VC} \gg \Gamma_1, \Gamma_2$, and the detuning is comparable to the decays rates, i.e., $|\omega - \omega_{CV}| \sim \Gamma_1, \Gamma_2$, we reach the fact that the main Fourier component of ρ_{VC} is oscillating at ω_{VC}, and the main Fourier component of ϱ is at dc. Therefore, the second term at the right-hand side of Eq. 2.4.27 contributes much less than the first term does. Dropping the second term of the right-hand side of Eq. 2.4.27, the interacting-matrix element is rewritten as

$$V_{VC} = -\mu_{VC} E e^{-i\omega t}, \tag{2.4.28}$$

which is known as the *rotating-wave approximation*. By use of the rotating-wave approximation, Eq. 2.4.26 can be solved analytically, giving the nonlinear susceptibility [60]

$$\chi = \frac{N\varrho^{eq}|\mu_{VC}|^2\Gamma_1\hbar(\omega - \omega_{VC} - i\Gamma_2)}{\Gamma_1\Gamma_2^2\hbar^2 + \Gamma_1\hbar^2(\omega - \omega_{VC})^2 + 4|\mu_{VC}|^2|E|^2\Gamma_2}. \tag{2.4.29}$$

Eq. 2.4.29 implies that for the resonant nonlinear susceptibility, saturation effect can be induced by a high-intensity field. Another consequence of Eq. 2.4.29 is that χ is composed of both a real part and an imaginary part. The real part contributes to a phase shift on the wave and the imaginary part causes absorption.

CHAPTER III

QUANTUM KEY DISTRIBUTION

The first part of my research focuses on improving the key-generation rate of current QKD systems. As discussed in Sec. 1.5, to improve the key-generation rate for QKD systems, one needs both new protocols and experimental techniques. This chapter covers a new QKD protocol and its experimental implementation, which provide a path for high-rate QKD systems. For the new QKD protocol, we adopt continuous-variable QKD (CVQKD) with discrete signaling and post selection. The purpose of discrete signaling and post selection is to allow use of low-complexity error-correction codes. Once the efficiency of the error-correction codes is much lower than the Shannon limit, the implementation complexity can be greatly reduced. In our experimental implementation, we use a continuous-wave local oscillator (CWLO) instead of the pulsed local oscillator that was used in [45]. We make quantum measurements at sidebands of the local oscillator. The bandwidth of detection can be as high as several hundred of MHz so that the large bandwidth of PiN detectors can be utilized. For fiber-based CWLO based systems, guided acoustic wave Brillouin scattering (GAWBS) is the main noise source to contaminate quantum signals. To avoid GAWBS noise, a novel experimental scheme was implemented based on frequency translation.

3.1 The protocol and security analysis

The two classes of CVQKD systems use continuous signaling [62, 63] and discrete signaling [64]. Continuous signaling, where Alice sends 2 independent Gaussian distributed random variables in the x and y quadratures of the field, is the most studied because proofs against individual and collective attacks exist [51–54]. An individual

attack describes manipulation of individual timeslots and optimal quantum measurement by Eve on light in that timeslot, while collective attacks describe manipulation of individual timeslots and optimal joint measurement of several or many timeslots. State-of-the-art continuously signaled experiments provide security against collective attacks, and demonstrate a final key rate of ~ 2 kbits/s [45]. This limitation is not due to the physical layer, but to the time required to execute reconciliation on a typical microprocessor. Attempts to increase speed have led to proposals for post selection, where only a subset of the received data is selected for error correction. By performing post selection, the required code efficiency and error rate can be manipulated. Recently, a protocol that can be proven secure against collective attacks is proposed if infinite dimensional conditional homodyne tomography can be implemented on a subset of data [56]. It has been clear to many CVQKD researchers that a discretely signaled CVQKD protocol would be advantageous in terms of simplicity and several protocols of this kind have been proposed. However, it has been pointed out that the security of discretely signaled systems under collective attacks remains an open problem for the practical case of excess noise in the channel [65]. Very recent work on the security of a binary modulated CVQKD system [55] showed quite limited tolerance to excess noise. However, we will show that the use of quantum tomography in a protocol can greatly improve the situation.

To increase distance, the technique of post selection has been proposed for CVQKD [66–69]. In post-selection schemes, only a subset of the data is used, improving the signal-to-noise ratio between Alice and Bob. CVQKD experiments have been implemented with post selection [67–69], but without security proofs. Although Gaussian attacks have been proved to be optimal against continuously signaled CVQKD systems, the optimal attack for post selection based CVQKD protocols is unknown yet. Recent progress on the security analysis of post selection [56] gave a proof of a post-selection protocol when excess Gaussian noise is introduced into the channel. The

protocol presented in their paper requires full conditional state tomography.

To permit faster and longer links, one needs to overcome the following obstacles. First, a very efficient reconciliation protocol is needed. Although theoretically, reverse reconciliation enables CVQKD links of infinite distance, as CVQKD link length increases, the minimum reconciliation efficiency required for positive secret-key capacity, β_0, approaches 1. This differs from discrete-variable QKD because in discrete-variable QKD, single photons and data sifting can efficiently bound eavesdropper's accessible information, and therefore highly efficient error-correction codes are not required. Second, reconciliation needs to be simple and fast. To correct errors between Alice and Bob, one usually seeks continuous-variable based error-correction codes to be as efficient as possible. However, highly efficient error-correction codes are also highly complex. We note that codes for binary symmetric channel are usually simpler. By turning the continuous-variable based error-correction problem into a binary based error-correction problem, several advantages come. First, it is easier to find corresponding error-correction codes whose efficiency is close to Shannon limit while keeping a lower decoding complexity. Furthermore, if the required error-correction efficiency is lowered for a given distance, then we may be able to find a reconciliation code with corresponding lower efficiency, which leads to lower decoding complexity. As a result, the distance and throughput of CVQKD systems would be significantly improved.

3.1.1 The quantized input-quantized output CVQKD protocol

According the previous discussions, binary reconciliation is attractive to improve CVQKD distance and key-generation rate. In 2006, Namiki proposed a CVQKD scheme using discrete encoding and post selection [64]. Although the protocol results in binary reconciliation, the security analysis was only developed for individual attacks. Furthermore, the experimentally relevant case of excess noise in the channel

was not treated. This case is important because system imperfections typically result in some additional noise, which should be treated for security purposes as if Eve controls it. For low channel efficiency, the possibility of selecting a quantum state is low enough that most of the measurements are discarded.

To obtain positive secret-key capacity, it is desirable that Alice and Bob nearly achieve the capacity of the channel given the signal-to-noise ratio. Recently, a new result of classical information theory [70] has shown that for a lossy Gaussian channel with given signal-to-noise ratio, when Bob quantizes the received data, the optimal way for Alice to encode data is to also send quantized data. Specifically, under the condition that Bob performs binary quantization, Alice needs only send binary data and achieve the channel capacity. This result is significant for reverse-reconciliation CVQKD because it indicates that if Bob quantizes the data received, then Alice does not need to send Gaussian modulated signals but should send binary signals. Since in a CVQKD protocol, we need to randomly switch between the X and Y quadrature, to make the two quadratures look symmetric under homodyne measurement, we at least need four coherent states. However, more coherent states lead to more complicated security analysis and experimental implementation. In this case, introducing four coherent states would be ideal for our purposes.

The quantized input-quantized output (QIQO) CVQKD protocol is described below:

Step 1: For each time slot, Alice randomly chooses a random variable $x_k \in \{1, 2, 3, 4\}$ and encodes a coherent state $|\alpha_{x_k}\rangle \in \{|\alpha_1\rangle = |r+ri\rangle, |\alpha_2\rangle = |r-ri\rangle, |\alpha_3\rangle = |-r+ri\rangle, |\alpha_4\rangle = |-r-ri\rangle\}$, where r is a positive real number depending on Bob's signal-to-noise ratio and k is the index of the time slot, and sends it through a lossy and noisy quantum channel. Alice's encoding scheme can be described in Figure 12.

Step 2: Bob receives a quantum state from the quantum channel. With probability p, the measurement is assigned to channel characterization, where Bob randomly

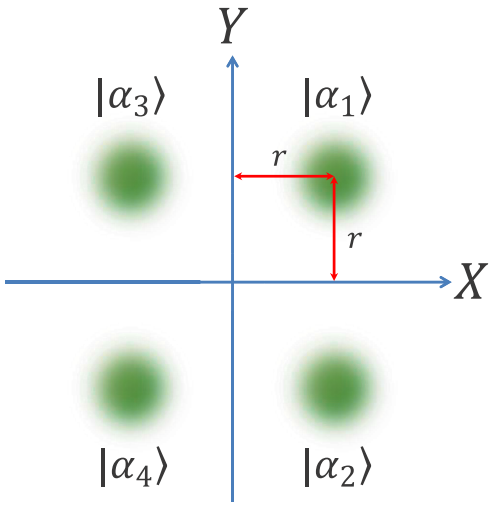


Figure 12: Alice's encoding scheme in which she only sends four different coherent states.

chooses a local oscillator phase ϕ_k of 0, $\pi/4$, or $\pi/2$, makes a homodyne measurement and records the real result [71]. With probability $1-p$, the measurement is assigned a data collection indexed by k, where Bob randomly chooses a local oscillator phase ϕ_k of 0 or $\pi/2$ and performs a homodyne measurement. If his measurement result is greater than T, where $T \geq 0$ is Bob's decision threshold, he quantizes the result to $q_k = 1$. If Bob's measurement result is less than $-T$, otherwise, he quantizes the data to $q_k = -1$. For other cases where his measurement result is between $-T$ and T, Bob quantizes his data to $q_k = 0$. When $q_k = 0$, the data from the corresponding time slot will not be selected in the post processing. When $T = 0$, the protocol reduces to the case without post selection.

To summarize these two steps, Alice uses random quadrature phase-shift keying (QPSK) signaling but Bob's collected data are digitized binary phase-shift keying (BPSK).

Step 3: When all quantum communication has been finished, Bob reveals to Alice which time slots were used for channel-characterization measurements. Alice then

reveals to Bob the state that she has sent for those time slots, after which Bob performs a conditional quantum tomography for each one of the four particular coherent states that Alice sent. We note here that conditional tomography is only practical for discrete-signaling based CVQKD protocols because in continuous-signaling CVQKD protocols, the size of Alice's signal set is infinity in principle. In practice, the size of Alice's signal set is limited by the resolution of Alice's D/A converter. For a 16-bit D/A converter, the size of Alice's signal set is 2^{16}, which makes it unrealistic to perform conditional tomography.

Only three different phases, 0, $\pi/4$, and $\pi/2$ in this protocol, are required to achieve a good estimate (fidelity higher than 99%) of the received state [71]. We know that without Eve, the channel can be modeled as a beamsplitter with two inputs, one of which is Alice's output to the quantum channel and the other one is the excess channel noise mode. In the Heisenberg picture, we have

$$\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{\varepsilon}_n, \tag{3.1.1}$$

where $\hat{b}$ is the output of the beamsplitter going to Bob's detectors and η is quantum efficiency of the quantum channel. For any field quadrature of Bob, we have

$$\hat{Q}_b = \sqrt{\eta}\hat{Q}_a + \sqrt{1-\eta}\hat{Q}_{\varepsilon_n}, \tag{3.1.2}$$

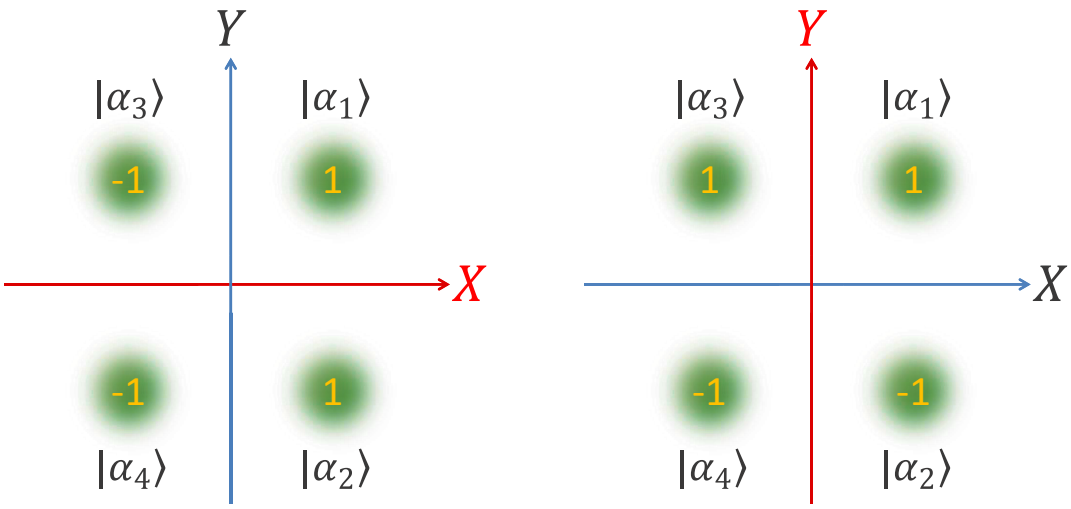
where $\hat{Q}_b$ is Bob's quadrature operator, $\hat{Q}_a$ is Alice's corresponding quadrature operator, and $\hat{Q}_{\varepsilon_n}$ is the corresponding quadrature operator of the noise mode. Assuming $p_b(q)$, $p_a(q)$ and $p_{\varepsilon_n}(q)$ are the probability distributions of the three quadratures, we have

$$p_b(q) = p_a(\sqrt{\eta}q) * p_{\varepsilon_n}(\sqrt{1-\eta}q), \tag{3.1.3}$$

where * is the linear convolution. By Fourier transform techniques, one can find $p_{\varepsilon_n}(q)$ once $p_a(q)$ and $p_b(q)$ are known from quantum tomography. By performing an inverse convolution, we can reconstruct the noise-mode density matrix $\hat{\rho}_{\varepsilon_n}$ based on

quantum tomography on Bob's density matrix $\hat{\rho}_b$. For the protocol, Bob performs quantum conditional tomography for all four cases. Then Bob can reconstruct $\hat{\rho}_{\varepsilon_n}$ for all four cases. The protocol requires that the reconstructed $\hat{\rho}_{\varepsilon_n}$ for all four cases to be identical. Otherwise, Alice and Bob abort the protocol.

Step 4: For each data-collection time slot, Bob reveals the local oscillator phase that was chosen. If Bob used $\phi_k = 0$, then Alice records $a_k = 1$ for the case $x_k = 1$ or $x_k = 2$ and $a_k = -1$ for the case $x_k = 3$ or $x_k = 4$. If Bob used $\phi_k = \frac{1}{2}\pi$, then Alice records $a_k = 1$ for the case $x_k = 1$ or $x_k = 3$ and $a_k = -1$ for the case $x_k = 2$ or $x_k = 4$. The decision rule is plotted in Figure 13.



(a) Alice's decision rule for $\phi_k = 0$

(b) Alice's decision rule for $\phi_k = \frac{\pi}{2}$

Figure 13: The decision of Alice for the data-collection time slots.

Step 5: Bob sends checkbits to Alice over a public channel, i.e. *reverse reconciliation*. The reconciliation is strictly one-way.

Step 6: Alice and Bob perform privacy amplification to distill the final secure key.

3.1.2 Security analysis

In this section, we analyze the security of the QIQO CVQKD protocol against collective attacks, where Eve interacts with incoming quantum states individually and makes joint multi-timeslot measurements after knowing Bob's measurement basis. The security of CVQKD systems can be guaranteed by fundamental limits of the noise coming from the quantum measurements. However, since the quantum channel can always introduce some excess noise, this amount of noise could potentially have been introduced by Eve, and may thus weaken the security of the system. In the security analysis, we will treat the excess channel noise rigorously. We divide this section into two subsections. In the first subsection, we analyze the simpler case where no excess channel noise exists but Bob's homodyne detector has a given quantum efficiency and Bob also has some additive Gaussian electronic noise. We will give an analytical solution for this case. In the second subsection, we analyze the case where measured excess noise is assumed to have a quantum channel as its source.

For collective attacks, the secret-key capacity between Alice and Bob per channel use is found by [50]

$$\Delta I = I(A;B) - \chi(B;E), \tag{3.1.4}$$

where $I(A;B)$ is the mutual information between Alice and Bob and $\chi(B;E)$ is the Holevo information between Bob and Eve. However, practical reconciliation codes do not reach the Shannon limit. The practical secret-key capacity in this case becomes

$$\Delta I = \beta I(A;B) - \chi(B;E). \tag{3.1.5}$$

To make the practical secret-key capacity positive so that Alice and Bob can distill a secure key by privacy amplification, a minimal required reconciliation efficiency β_0 exists where

$$\beta_0 I(A;B) - \chi(B;E) = 0. \tag{3.1.6}$$

For the binary symmetric channel in our protocol, $I(A;B)$ in bits can be completely

determined by the signal-to-noise ratio (SNR), which will be defined rigorously later, of Bob. $I(A;B)$ relates to the bit error rate e_{AB} on the binary symmetric channel by

$$e_{AB} = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\sqrt{\text{SNR}}} e^{-\frac{x^2}{2}} dx. \tag{3.1.7}$$

$$I(A;B) = 1 - h(e_{AB}), \tag{3.1.8}$$

where $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary entropy function.

the Holevo information between Bob and Eve is defined as

$$\chi(B;E) = S(\hat{\rho}_E) - \sum_i p_i S(\hat{\rho}_{E|q=i}), \tag{3.1.9}$$

where $S(\hat{\rho}_E)$ is the von Neumann entropy of Eve's mixed state $\hat{\rho}_E$, $\hat{\rho}_{E|q=i}$ is Eve's mixed state given Bob's measurement result, and p_i is the probability that Bob's measurement is i. For our binary symmetric case, we can rewrite $\chi(B;E)$ to be

$$\chi(B;E) = S(\hat{\rho}_E) - \frac{1}{2}S(\hat{\rho}_{E|q=-1}) - \frac{1}{2}S(\hat{\rho}_{E|q=1}) = S(\hat{\rho}_E) - S(\hat{\rho}_{E|q=1}) \tag{3.1.10}$$

for an optimal attack.

When no excess channel noise exists, Bob's received state is a coherent state given Alice sent a particular quantum state. When the tomographic subset verifies Bob's received state, Eve's only possible attack is a beam splitter attack, where Eve replaces the lossy channel with a perfect one and uses a beam splitter to simulate the lossy effect of the channel. Suppose the quantum efficiency of the quantum channel is η, then Bob's received quantum states are $|\sqrt{\eta}\alpha_i\rangle$ and Eve's received quantum states are $|\sqrt{1-\eta}\alpha_i\rangle$, given Alice sent $|\alpha_i\rangle$. It is straight forward to give the expression for $\hat{\rho}_E$:

$$\hat{\rho}_E = \sum_{i=1}^{4} \frac{1}{4} |\sqrt{1-\eta}\alpha_i\rangle\langle\sqrt{1-\eta}\alpha_i|. \tag{3.1.11}$$

The second term of $\chi(B;E)$ relates directly to the error rate of the binary symmetric channel. Let us consider the case where Bob chose $\phi = 0$ as the phase for homodyne detection. Given Bob's quantized data $q = 1$, the possibility that Alice sent

$|\alpha_1\rangle$, $|\alpha_2\rangle$, $|\alpha_3\rangle$, and $|\alpha_4\rangle$ are $p_{1|q=1} = \frac{1}{2}(1 - e_{AB})$, $p_{2|q=1} = \frac{1}{2}e_{AB}$, $p_{3|q=1} = \frac{1}{2}(1 - e_{AB})$, and $p_{4|q=1} = \frac{1}{2}e_{AB}$ respectively. Therefore, the conditional density matrix

$$\hat{\rho}_{E|q=1} = \sum_{i=1}^{4} p_{i|q=1} |\sqrt{\eta - 1}\alpha_i\rangle\langle\sqrt{\eta - 1}\alpha_i|. \tag{3.1.12}$$

The error rate e_{AB} is related to the signal-to-noise ratio of Bob by 3.1.7. Suppose the vacuum variances of both quadratures are $\langle\Delta X^2\rangle = \langle\Delta Y^2\rangle = V_S = \frac{1}{4}$ and the variance of electronic noise is V_{el}, then the variance of Bob's measurement noise, including both the quantum noise arising from the homodyne measurement and the electronic noise arising from the experimental circuits such as electronic amplifier, is

$$V_B = V_S + V_{\text{el}}. \tag{3.1.13}$$

The signal-to-noise ratio reads

$$\text{SNR} = \frac{u_i^2}{V_B}, \tag{3.1.14}$$

where $u_i = \Re\{\sqrt{\eta\eta_m}\alpha_i\}$ is Bob's expected value of the X quadrature given Alice sent α_i. η_m is the detection efficiency of the homodyne detector. Combining Eq. 3.1.13 and Eq. 3.1.14, we have

$$\text{SNR} = \frac{\Re^2\{\sqrt{\eta\eta_m}\alpha_i\}}{V_B} = \frac{\eta\eta_m r^2}{V_B}. \tag{3.1.15}$$

Together with Eq. 3.1.7, we can calculate the error rate of the binary symmetric channel between Alice and Bob. Combining the above equations, we get the analytical expression for the secret-key capacity between Alice and Bob for the case where no excess noise exists.

In the case where excess noise is introduced into the quantum channel, the analysis is more complicated and numerical simulations are required. We will prove that with small amounts of excess noise, the security of the QIQO CVQKD scheme can still be guaranteed. The details of the numerical simulation are reported in appendix A.

3.1.2.1 Validity of channel model

We will show that Eve's optimal collective attack is the entangling beamsplitter attack (see Figure 14), where Eve replaces the lossy fiber with a lossless channel and mixes one of two entangled beams ($\hat{\rho}_{\varepsilon_n}$) on a beamsplitter while additionally monitoring one of the outputs ($\hat{\rho}_{\varepsilon_r}$). *Conditional* homodyne tomography serves to make the optimality of the entangled beamsplitter attack provable.

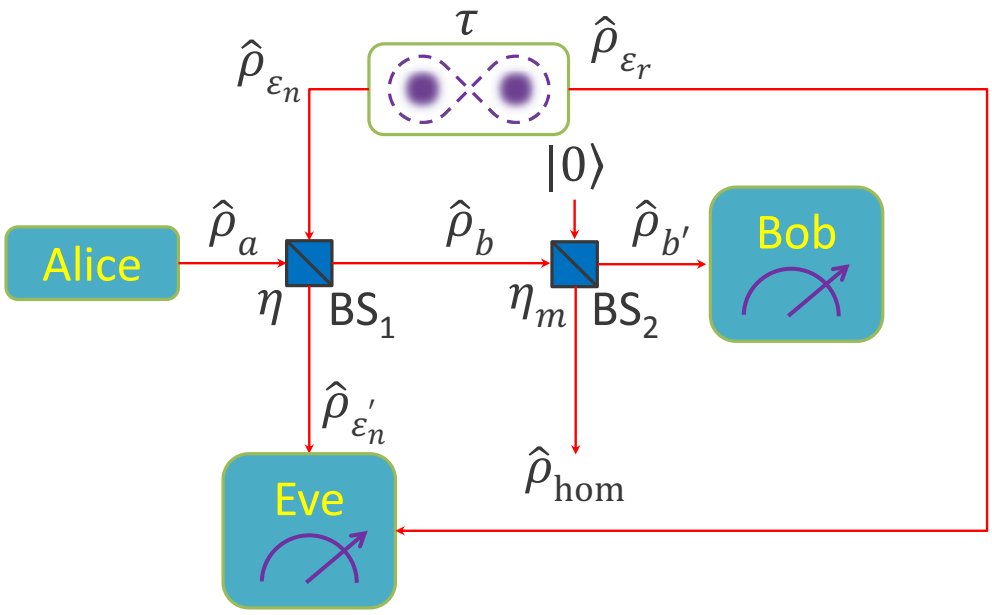


Figure 14: Model of the relevant quantum channel. $\hat{\rho}_{\varepsilon_n}$ and $\hat{\rho}_{\varepsilon_r}$, density matrices produced by Eve's EPR source; $\hat{\rho}_a$, density matrix of the signal sent by Alice; $\hat{\rho}_b$ and $\hat{\rho}_{b'}$, density matrix before Bob's detector inefficiencies and after detector inefficiencies; $\hat{\rho}_{\varepsilon_{n'}}$, density matrix post BS$_1$, measured by Eve; $\hat{\rho}_{\text{hom}}$, density matrix of equivalent mode consisting of light lost to detector inefficiencies. τ is the squeezing parameter of the EPR source, η is the channel efficiency, and η_m is Bob's detector efficiency.

We need to note that Eve's attack is a unitary operator which maps the product state of Eve's original ancillary state ρ_{ε_n} and Alice's output state ρ_a to the state ρ_b,

which is measured by Bob's detectors and to the final ancillary state. If the input ancillary state and Alice's output state are given, and the output states of the unitary operator are also given, then the unitary operator can be regarded as a black box. In this case, the internal structure of the black box does not matter because the secret-key capacity of the system is only a function of the output of the black box. In other words, only the output quantum state matters and how the state was generated does not. Eve's unitary operation can be denoted as

$$|\Phi_i\rangle = \hat{M}(|\Psi_E\rangle \otimes |\alpha_i\rangle), \tag{3.1.16}$$

where $|\alpha_i\rangle$ denotes Alice's chosen state and $|\Psi_E\rangle$ denotes Eve's original ancillary states. Then Bob's incoming density matrices are given by a trace over Eve's Hilbert space

$$\rho_{b_i} = \mathrm{Tr}_E(|\Phi_i\rangle\langle\Phi_i|). \tag{3.1.17}$$

We know that ρ_{b_i} can be obtained by quantum conditional tomography and according to Eq. 3.1.1, each $\hat{b}_i$ can be expressed as a superposition of Alice's mode and another excess noise mode, we can decompose $\hat{M}$ into three different unitary operators $\hat{O}$, $\hat{P}$, and $\hat{Q}$. $\hat{O}$ creates $\hat{\rho}_{\varepsilon_n}$ from Eve's original ancillary states

$$\hat{\rho}_{\varepsilon_n} = \mathrm{Tr}_r[\hat{O}(|\Psi_E\rangle\langle\Psi_E|)\hat{O}^\dagger], \tag{3.1.18}$$

where Tr_r denotes the trace over the rest Eve's state besides mode ε_n. The role of operator $\hat{P}$ is to interact $\hat{\rho}_{\varepsilon_n}$ with $|\alpha_i\rangle$ on a beamsplitter to create ρ_{b_i}. $\hat{P}$ can be written as

$$\hat{P} = \begin{bmatrix} -\sqrt{\eta} & \sqrt{1-\eta} \\ \sqrt{1-\eta} & \sqrt{\eta} \end{bmatrix}. \tag{3.1.19}$$

The role of $\hat{Q}$ is to map the final state back to $|\Phi_i\rangle$. We have

$$\hat{Q} = \hat{M}\hat{O}^\dagger\hat{P}^\dagger. \tag{3.1.20}$$

Since for each of the four cases, either $\hat{M}$ or the cascading of $\hat{O}$, $\hat{P}$, and $\hat{Q}$ gives $|\Psi_i\rangle$ as the output quantum state, the decomposition is therefore equivalent to the unitary operator $\hat{M}$. The idea of the decomposition can be found in Figure 15.

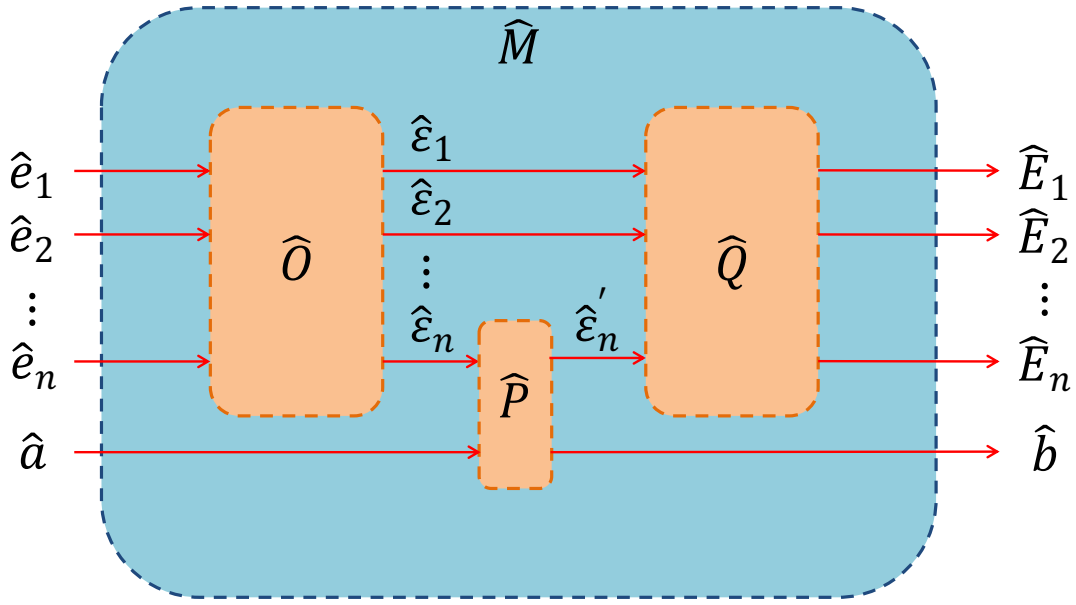


Figure 15: Eve's attack operator $\hat{M}$ can be decomposed into three sub-operators $\hat{O}$, $\hat{P}$, and $\hat{Q}$, which give identical output quantum states.

We note here that the operator $\hat{Q}$ is a post processing on Eve's states. According to the quantum data processing theorem [72], this operation does not increase Eve's accessible information. Therefore, we can safely only consider the system without $\hat{Q}$ since $\hat{Q}$ can only decrease Eve's accessible information. In other words, considering ρ_{ε_r} and $\rho_{\varepsilon'_n}$ is enough to evaluate Eve's accessible information.

When excess noise is present, for each of the coherent states Alice sends, Bob receives a state with less mean photon number but larger variance (see Figure 16). The decrease in mean is caused by channel loss while the increase in variance arises

from excess noise. Bob's conditional quantum state $\hat{\rho}_{B||\alpha_1\rangle}$ can be reconstructed by quantum conditional tomography. Knowing Bob's conditional quantum state, one is able to reconstruct Eve's quantum state and thus bound her accessible information.

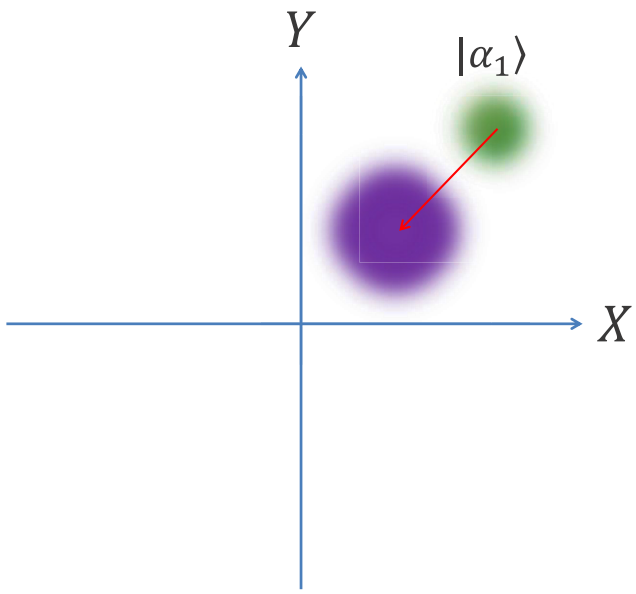


Figure 16: The effect of a noisy quantum channel. The green area represents Alice's sent coherent state, which turns into Bob's received state in the purple area.

As an example, we calculate a representative case where the excess channel noise is thermal. If the channel noise is not thermal, as long as we reconstruct $\hat{\rho}_{\varepsilon_n}$, we will be able to use the same method to calculate the secret-key capacity. In Figure 14, $\hat{\rho}_{\varepsilon_n}$ is Eve's input mode to the operator $\hat{P}$. Whatever Bob's state $\hat{\rho}_b$ is, he can reconstruct Eve's state $\hat{\rho}_{\varepsilon_n}$ because he has been told Alice's sent state $\hat{\rho}_a$. Mathematically, the thermal state $\hat{\rho}_{\varepsilon_n}$ can be written as

$$\hat{\rho}_{\varepsilon_n} = (1-\tau^2)\sum_{n=0}^{\infty}\tau^{2n}|n\rangle\langle n|. \tag{3.1.21}$$

In the Schrödinger picture, we let Eve's State to be in the pure state $|\Psi\rangle_{\varepsilon_n,\varepsilon_r}$, where the subscript ε_r denotes the rest of Eve's modes besides ε_n. One should note that although the notation here looks like Eve is using a two-mode state, Eve is not

limited to the number of modes. The quantum tomography guarantees that input mode ε_n to BS_1 to be a thermal state. Since Eve's entire quantum state is pure, the condition

$$\hat{\rho}_{\varepsilon_n} = \mathrm{Tr}_{\varepsilon_r}(|\Psi\rangle_{\varepsilon_n,\varepsilon_r\varepsilon_n,\varepsilon_r}\langle\Psi|), \tag{3.1.22}$$

must be satisfied. Without loss of generality, one can let $|\Psi_{\varepsilon_n,\varepsilon_r}\rangle$ be in the form

$$|\Psi_{\varepsilon_n,\varepsilon_r}\rangle = \sqrt{1-\tau^2}\sum_{n=0}^{\infty}\tau^n|n\rangle_{\varepsilon_n}|\phi(n)\rangle_{\varepsilon_r}, \tag{3.1.23}$$

where $\langle\phi(n)|\phi(n')\rangle = \delta_{n,n'}$.

Similar to other security proofs for CVQKD protocols, we adopt an entanglement-based picture by assuming Alice first prepares a two-mode quantum state

$$|\psi_A\rangle = \sum_{i=1}^{4}\frac{1}{2}|\alpha_i\rangle_a|i\rangle_{a'}. \tag{3.1.24}$$

In mode a', the state is expressed in the Fock basis and in mode a the state is written in the coherent basis. Alice then makes a photon-number-counting measurement on mode a', which projects the state of mode a into one of the four coherent states, i.e., $\hat{\rho}_a = \mathrm{Tr}_{a'}(|\psi_A\rangle\langle\psi_A|) = \sum_{i=1}^{4}\frac{1}{4}|\alpha_i\rangle_{aa}\langle\alpha_i|$, coinciding with the case where Alice randomly chooses one of the four coherent states and sends it through the quantum channel. The quantum state of the entire system becomes

$$|\Phi\rangle = \hat{B}_1(\eta)\hat{B}_2(\eta_m)|\psi_A\rangle|\Psi_{\varepsilon_n,\varepsilon_r}\rangle|0\rangle_{\mathrm{hom}}, \tag{3.1.25}$$

where $\hat{B}_1(\eta_m)$ and $\hat{B}_2(\eta)$ denote the unitary operator of BS_1 and BS_2.

Bob then makes a homodyne measurement on mode b'. Each measurement result, according to the state-reduction postulate of quantum mechanics, collapses the rest of the system into a pure quantum state. Suppose Bob's homodyne measurement results in a real-valued number X, the rest of the system collapses into the state

$$|\Xi^X\rangle = \frac{{}_{b'}\langle X|\Phi\rangle}{\sqrt{\langle\Phi|X\rangle_{b'b'}\langle X|\Phi\rangle}}, \tag{3.1.26}$$

Tracing over Alice's mode a' and mode hom, one obtains Eve's density matrix given the measurement result X:

$$\hat{\rho}_E^X = \mathrm{Tr}_{a',\mathrm{hom}}(|\Xi^X\rangle\langle\Xi^X|). \tag{3.1.27}$$

The probability that $\hat{\rho}_E^X$ is produced is

$$p(\hat{\rho}_E^X) = \langle\Phi|X\rangle_{b'b'}\langle X|\Phi\rangle. \tag{3.1.28}$$

Eve's overall density matrix $\hat{\rho}_E$ can be derived by

$$\hat{\rho}_E = \int p(\hat{\rho}_E^X)\hat{\rho}_E^X dX \tag{3.1.29}$$

Realistically, homodyne measurements with additive classical electronic noise leads to a real-valued measurement result $r_B = X + N_{\mathrm{el}}$, which is the sum of X, from the quantum measurement, and N_{el}, a Gaussian distributed random variable arising from the electronic noise. *Without* post selection, the protocol requires that Bob quantizes r_B to its sign, either 1 or -1. If $r_B > 0$ Bob sets the quantized bit $q = 1$. Otherwise, Bob lets the quantized bit be $q = -1$. To obtain $\chi(B;E)$, we are interested in the conditional density matrix of Eve given Bob's quantization result. Without loss of generality, we only analyze the case in which $q = 1$.

Because the overall system state is a pure state until Bob performs quantum measurement, Eve's density matrix is a function of Bob's homodyne measurement result X. However, Bob's quantization result not only depends on X, but also depends on N_{el}, an independent random variable from of X. We can regard Eve's conditional density matrix $\hat{\rho}_{E|q=1}$ as the superposition of different $\hat{\rho}_E^X$ weighting their probabilities $p(\hat{\rho}_E^X|q=1)$. Therefore, Eve's conditional density matrix can be written as

$$\hat{\rho}_{E|q=1} = \int p(\hat{\rho}_E^X|q=1)\hat{\rho}_E^X dX., \tag{3.1.30}$$

where $p(\hat{\rho}_E^X|q=1)$ is given by Bayes' theorem:

$$p(\hat{\rho}_E^X|q=1) = \frac{p(\hat{\rho}_E^X)p(q=1|\hat{\rho}_E^X)}{p(q=1)}, \tag{3.1.31}$$

where $p(\hat{\rho}_E^X)$ is obtained by Eq. 3.1.28, and Alice's symmetric signaling leads to $p(q=1)=\frac{1}{2}$. $p(q=1|\hat{\rho}_E^X)$ depends on V_{el}, the electronic-noise variance:

$$p(q=1|\hat{\rho}_E^X)=\frac{1}{\sqrt{2\pi V_{\text{el}}}}\int_{-\infty}^{X}\exp\left(-\frac{x^2}{2V_{\text{el}}}\right)dx. \tag{3.1.32}$$

Next we derive e_{AB}, based on which $I(A;B)$ can be obtained. According to Eq. 3.1.7, to obtain e_{AB}, we have to calculate the signal-to-noise ratio of Bob. When the quantum channel is introduced with some excess thermal noise, Bob's measurement noise is made up of three parts: the quadrature noise with variance $\frac{1}{4}$, the electronic noise with variance V_{el}, and the thermal noise whose variance depends on τ, the squeezing factor of Eve's EPR source, and η, the quantum efficiency of the channel. Let the mean thermal photon number be

$$\langle n_{th}\rangle=(1-\tau^2)\sum_{n=0}^{\infty}n\tau^{2n}=\frac{\tau^2}{1-\tau^2}. \tag{3.1.33}$$

Bob's noise variance reads

$$V_B=V_S+\frac{1}{2}(1-\eta)\eta_m\langle n_{th}\rangle+V_{\text{el}}. \tag{3.1.34}$$

Using Eq. 3.1.34 and Eq. 3.1.14, we can obtain the expression for the signal-to-noise ratio for the case with excess noise:

$$\text{SNR}=\frac{\Re^2\{\sqrt{\eta\eta_m}\alpha_i\}}{V_S+\frac{1}{2}(1-\eta)\eta_m\frac{\tau^2}{1-\tau^2}+V_{\text{el}}}=\frac{\eta\eta_m r^2}{V_B}. \tag{3.1.35}$$

The practical limitation on the key generation rate of CVQKD systems is the decoding complexity for reconciliation. Treating the channel as if it was a binary symmetric channel for reconciliation purposes, the complexity of error correction codes used in reconciliation decreases. Suppose that for a given code, the code length is N and the code rate is $R=(1-\varepsilon)C$, where C is the channel capacity, in this case decoding time complexity is a function of ε and N. Typically, it grows polynomially with N. It has also been conjectured in [73] that per-bit complexity of message-passing decoding of LDPC code over any "typical" channel, such as a binary erasure channel

or a binary symmetric channel, is $O(\log \frac{1}{\pi}) + O(\frac{1}{\varepsilon} \log \frac{1}{\varepsilon})$, where π is the decoding error rate. So the closer the code approaches the Shannon limit, the more complex the code is. In other words, the requirement of high β_0 leads to very complex codes. Even so, the decoding error probability drops only polynomially with code length for LDPC codes, which requires even more time complexity to reduce the block error rate to suitable levels.

For the proposed QIQO CVQKD scheme, to have positive secret-key capacity, Bob's signal-to-noise ratio must be very low, i.e., around 0.5, which causes e_{AB} to be very high, i.e., around 25%. To fit the error rate to the requirements of those low-complexity codes, we need to modify e_{AB} while also changing β_0 little. Post selection satisfies these requirements.

Bob's final measurement result is $r_B = X + N_{\text{el}}$ if electronic noise is included. According to the protocol, if $r_B > 0$, Bob quantizes it to $q = 1$. Otherwise, Bob quantizes it to $q = -1$. With post selection, we set a threshold $T > 0$. Bob's quantization rule is modified as follows: for the case $r_B > T$, he sets $q = 1$, for the case $-T \leq r_B \leq T$, he sets $q = 0$, and for the case $r_B < -T$, he sets $q = -1$. Finally, Alice and Bob discard data where $q = 0$ and only make error correction on the data where $q \neq 0$. Bob's decision rule for post selection can be visualized in Figure 17.

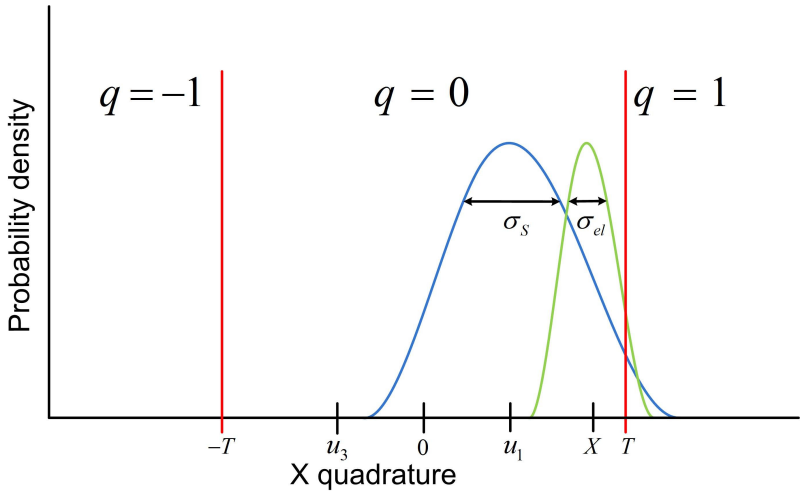


Figure 17: Bob's decision rule under post selection. $\sigma_S = \sqrt{V_S}$ **and** $\sigma_{\text{el}} = \sqrt{V_{\text{el}}}$**.**

To derive for $\hat{\rho}_E$ under post selection, we need to reevaluate the probability for each $\hat{\rho}_E^X$. We denote the new probability as $p(\hat{\rho}_E^X|q \neq 0)$. Using Bayes' theorem

$$p(\hat{\rho}_E^X|q \neq 0) = \frac{p(q \neq 0|\hat{\rho}_E^X)p(\hat{\rho}_E^X)}{p(q \neq 0)} \tag{3.1.36}$$

The first term of the numerator is obtained by

$$p(q \neq 0|\hat{\rho}_E^X) = \frac{1}{\sqrt{2\pi V_{\text{el}}}} \left[\int_{-\infty}^{-(T-X)} \exp\left(-\frac{x^2}{2V_{\text{el}}}\right) + \int_{-\infty}^{-(T+X)} \exp\left(-\frac{x^2}{2V_{\text{el}}}\right) \right] dX. \tag{3.1.37}$$

The second term of the numerator is evaluated by Eq. 3.1.28. The denominator is the probability of keeping a result. It directly relates to the amplitude of the signal u_i, the measurement-noise variance V_B, and the decision threshold T:

$$p(q \neq 0) = \frac{1}{\sqrt{2\pi V_B}} \left[\int_{-\infty}^{-(T-u_i)} \exp\left(-\frac{x^2}{2V_B}\right) + \int_{-\infty}^{-(T+u_i)} \exp\left(-\frac{x^2}{2V_B}\right) \right] dx. \tag{3.1.38}$$

$\hat{\rho}_E$ can be therefore written as

$$\hat{\rho}_E = \int p(\hat{\rho}_E^X|q \neq 0)\hat{\rho}_E^X dx. \tag{3.1.39}$$

To bound Eve's accessible information, one must next evaluate $p(\hat{\rho}_E^X|q = 1)$ by Eq. 3.1.31. The first term on the numerator equals Eq. 3.1.28. The second term of the numerator is reformulated by

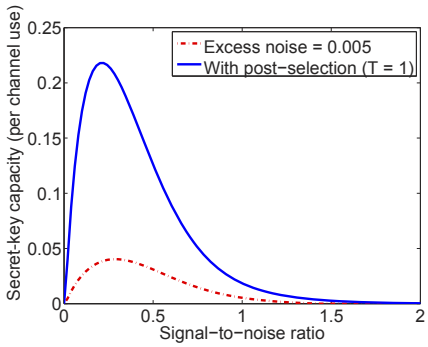
$$p(q = 1|\hat{\rho}_E^X) = \frac{1}{\sqrt{2\pi V_{\text{el}}}} \int_{-\infty}^{-(T-X)} \exp\left(-\frac{x^2}{2V_{\text{el}}}\right) dx. \tag{3.1.40}$$

Having obtained the preceding probabilities, we obtain $\chi(B;E)$ according to Eq. 3.1.10.

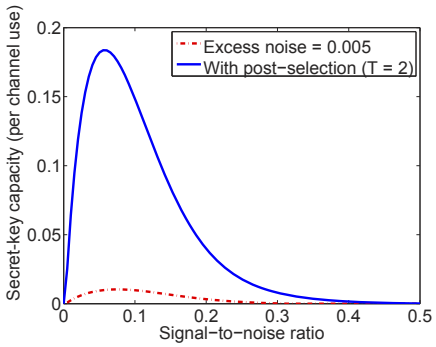
In the last step, we examine e_{AB} under post selection to derive the mutual information $I(A;B)$. The symmetry of the states implies that the error rate is a constant regardless of Alice's sent state $|\alpha_i\rangle$. For simplicity, we only calculate the error rate when Alice encodes $|\alpha_1\rangle$:

$$\begin{aligned} e_{AB} &= \frac{p(q = -1|\text{Alice encodes}|\alpha_1\rangle)}{p(q \neq 0)} \\ &= \frac{\int_{-\infty}^{-(T+u_i)} \exp\left(-\frac{x^2}{2V_B}\right) dx}{\int_{-\infty}^{-(T-u_i)} \exp\left(-\frac{x^2}{2V_B}\right) dx + \int_{-\infty}^{-(T+u_i)} \exp\left(-\frac{x^2}{2V_B}\right) dx}. \end{aligned} \tag{3.1.41}$$

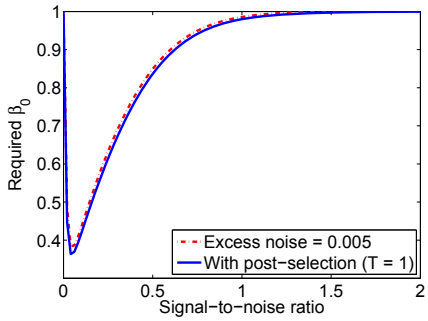
The secret-key capacity under post selection is obtained straightforwardly by evaluating Eq. 3.1.5. We present numerical simulation results and compare them to the case without post selection in Figure 18. We note that the post selection does not require



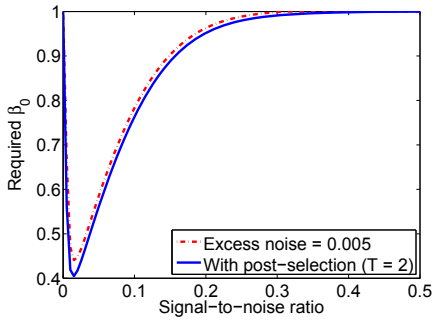
(a) The secret-key capacity of the system with post selection at 25 km



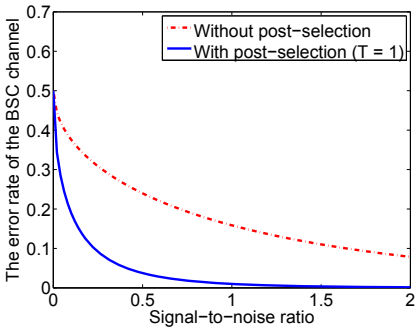
(b) The secret-key capacity of the system with post selection at 50 km



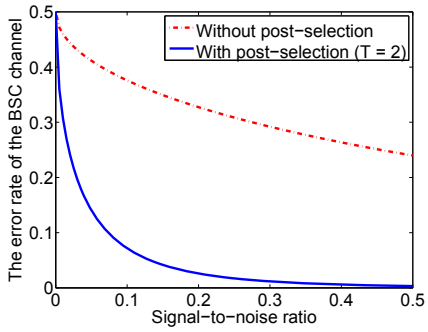
(c) The required β_0 for the system with post selection at 25 km



(d) The required β_0 for the system with post selection at 50 km



(e) The error rate of the BSC channel at 25 km



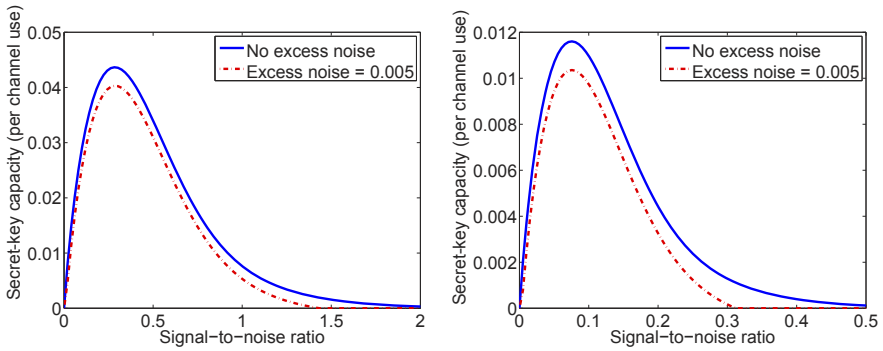
(f) The error rate of the BSC channel at 50 km

Figure 18: A comparison on the secret-key capacity, the required reconciliation efficiency, and the error rate and the BSC channel for the protocol with and without post selections. Excess noise in quantum units.

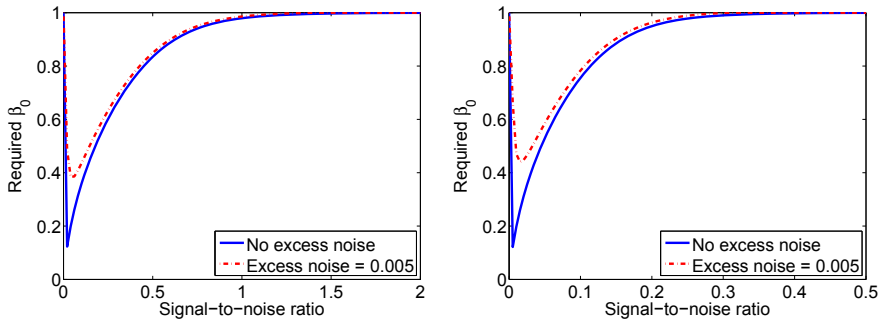
high rate multi-bit A/D conversion. It only requires a low-cost threshold decision gate. For the case where $T = 1$, around 10% of the data is selected. Therefore, if the clock rate is high enough, post selection will not be the bottleneck that limits the key-generation rate.

3.1.2.2 Discussion of results

Numerical simulation results of the secret-key capacity and the required reconciliation efficiency with and without post selection are presented in Figure 19.



(a) The secret-key capacity for 25 km (b) The secret-key capacity for 50 km



(c) The required reconciliation efficiency β_0 for 25 km (d) The required reconciliation efficiency β_0 for 50 km

Figure 19: The secret-key capacity and required reconciliation efficiency for the system without post selection. Excess noise in quantum units.

Several observations are in order. First, as expected, it is clear that excess noise reduces secret-key capacity and increases β_0. This is as expected because we assumed that Eve could make use of the excess noise and thus achieve higher mutual

information with Bob. Secondly, it is also clear why β_0 increases with increasing signal-to-noise ratio. This is because at higher SNRs, the signal amplitude increases, which leads Eve to better discrimination between the four states sent by Eve. To take advantage of coding, we require a relatively low β_0 and thus we require error-correction codes that work at low SNRs. However, at low SNRs, the error probability of the binary symmetric channel increases. As discussed previously, very good codes have been found for binary symmetric channels but they are very sensitive to the error probability of the channel. To make those codes applicable to our case, we use post selection on Bob's received data so that the secret-key capacity (per retained bit) between Alice and Bob increases dramatically, the error probability (per retained bit) drops dramatically, while the required β_0 remains almost constant. For 25 km QIQO CVQKD, a threshold of $T = 1$ is set for post selection. This leads to post selection of 10% of Bob's data. For 50 km QIQO CVQKD, a threshold $T = 2$ leads to retention of about 1% of Bob's data. For 25 km QIQO CVQKD with post selection, the ideal working region is at a signal-to-noise ratio about 0.25, where the secret-key capacity is 0.2 bits/channel use, the error probability is less than 10% and the required β_0 is about 60%. For 50 km QIQO CVQKD, the ideal working region is at signal-to-noise ratio about 0.15, where the secrecy capacity is 0.15 bits/channel use, the error probability is less than 10% and the required β_0 is about 75%.

In Figure 20, we plot the key-generation rate vs distance. We set the clock rate to be 10 MHz, channel loss be 70%, $\beta = 80\%$, $e_{AB} = 7\%$ and excess noise from the source be 0.005 shot-noise units. The detected excess noise is $0.005 \times V_S \eta \eta_m = 0.0011$ quantum units. The numerical result shows that at 25 km, we achieve 100 kbit/s key-generation rate. At 50 km, positive secret-key capacity around 100 bit/s still exists. The numerical simulation is accurate up to 60 km, after which the numerical sensitivity limit is reached.

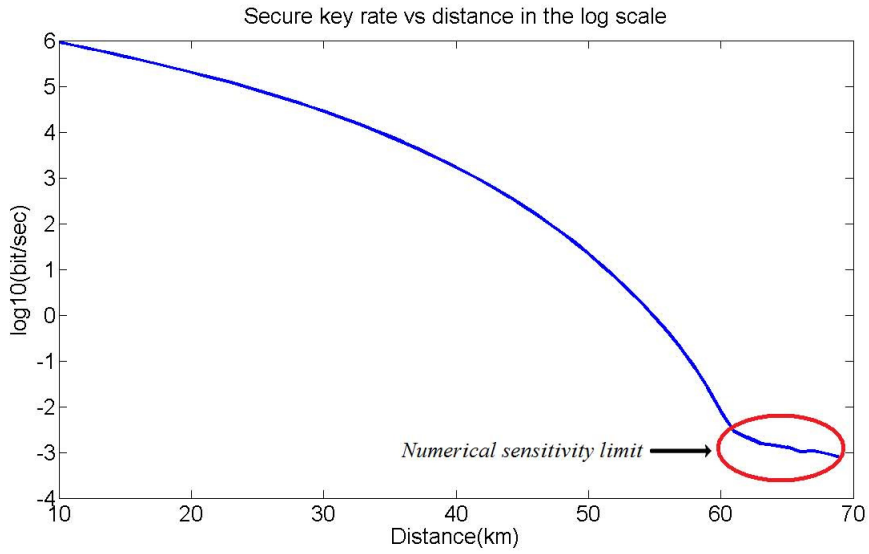


Figure 20: The key-generation rate vs distance.

We have also made initial simulations on a simple error correction code and compared the results to previous CVQKD experiments without post selection. For 25 km QKD, after the post-selection process, we have an error rate about 7% on the BSC channel. We then use a standard unoptimized LDPC code that corrects all the errors. Running on a Mac laptop, one may decode at a processing rate of 600 kbit/s at a reconciliation efficiency of $\beta = 80\%$. The secret key rate per channel use when we take the inefficiency of the error correction code into account is $\Delta I = \beta I(A;B) - \chi(B;E) = 0.1$ at 25 km at signal-to-noise ratio 0.45. This results after privacy amplification in a final key rate of 60 kbps at 25 km with channel loss 70%. This provides a speed up by a factor of 25 over the existing experiment that uses a protocol secure against collective attacks.

A security analysis on binary modulated CVQKD system has been posted [55] after we presented most of these results [74]. That protocol uses two-state modulation instead of four-state modulation. It does not require quantum tomography. Instead, inequalities and maximum eigenvalues are found to get a upper bound for Eve. The inequalities result in an upper bound less tight than that found in this work, which

makes that protocol more sensitive to channel excess noise. We also compare our result with [69], which is limited to 50 km with no excess noise. But the scheme proposed in this work is secure beyond 50 km with realistic excess noise and still has high secret-key capacity.

3.2 Quantum key distribution experiment using a continuous-wave local oscillator

In this section, we describe an experimental implementation of the proposed continuous-variable QKD protocol. Some currently reported CVQKD experiments are implemented in optical fiber [45, 75, 76] and others simulate a lossy channel with a beamsplitter [68, 69, 77, 78]. Compared to previous work, this is the first experiment to use discrete signaling over optical fiber with a security proof. It is also the first CVQKD system that uses a CWLO over fiber, which we believe to be better suited for higher speed systems. To achieve this we implement a frequency translation scheme that avoids guided acoustic wave Brillouin scattering (GAWBS) [79], an effect which otherwise contaminates the signal by scattering light from the orthogonally polarized LO. We believe this work is significant as well for potential pulsed CVQKD systems where GAWBS noise could be present at pulse rates as low as tens of MHZ. This work is also the first QKD experiment to use optical amplifier in the receiver for amplification of the LO.

3.2.1 Experimental setup and calibration process

The idea of the frequency translation scheme is schematically represented in Figure 21, where the LO and signal are ready to be combined on 50/50 fiber coupler BS in Figure 23 before detection. We first describe the preparation of the frequency translated signal by Alice by devices shown in the box labeled “Alice” in Figure 23. After separation of the LO from the signal by a 99/1 coupler, phase modulator PM2 sets the QPSK modulation, the phase shift between the LO and quantum signal.

The signal, after the separation from the LO by the 99/1 coupler and attenuation by attenuator A, is placed in 50 MHz sidebands by amplitude modulator AM to avoid baseband noise of the LO in final detection. By biasing AM near the extinction point, the signal light is placed entirely into two sidebands. Next, the signal is frequency translated by phase modulator PM1. The drive voltage for PM1 is chosen so that the phase shift amplitude ϕ corresponds to the first root of the Bessel function $J_0(\phi)$. The result is that the signal light is ideally entirely frequency shifted away from the optical LO frequency, creating sidebands spaced 2 GHz apart. PM1 and PM2 are separate to safely limit the RF power per modulator. The LO and the signal are combined on a polarization beam splitter (PBS1) then sent to the transmission channel fiber with linear loss of 5.18 dB.

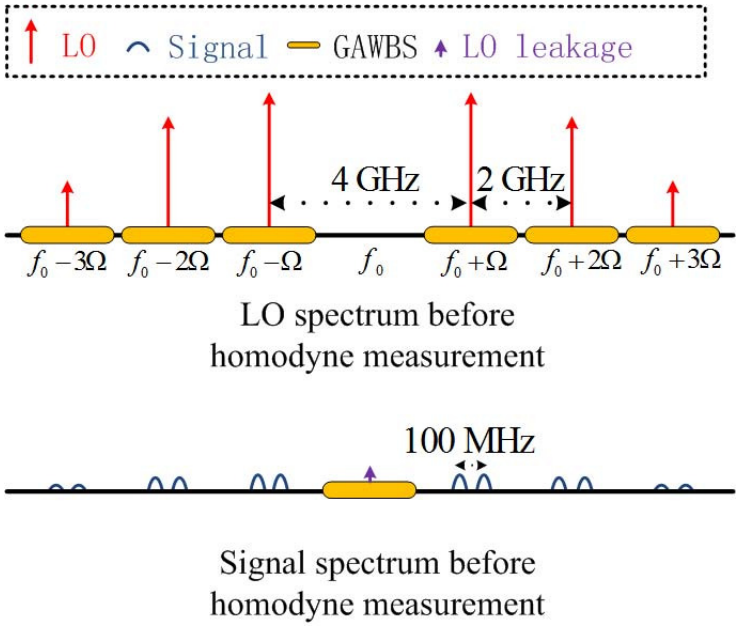


Figure 21: (top) Final LO spectrum before homodyne detection. (bottom) Final signal spectrum before homodyne detection.

In the fiber, guided acoustic wave Brillouin scattering (GAWBS) causes a portion of the LO to scatter into frequencies up to 1.8 GHz. These frequencies correspond to thermally populated acoustical phonon modes in the fiber that modulate the refractive

index of the fiber core. The scattering is composed of both co-polarized and de-polarized components. The measured spectrum of GAWBS noise in our experiment is shown in Figure 22.

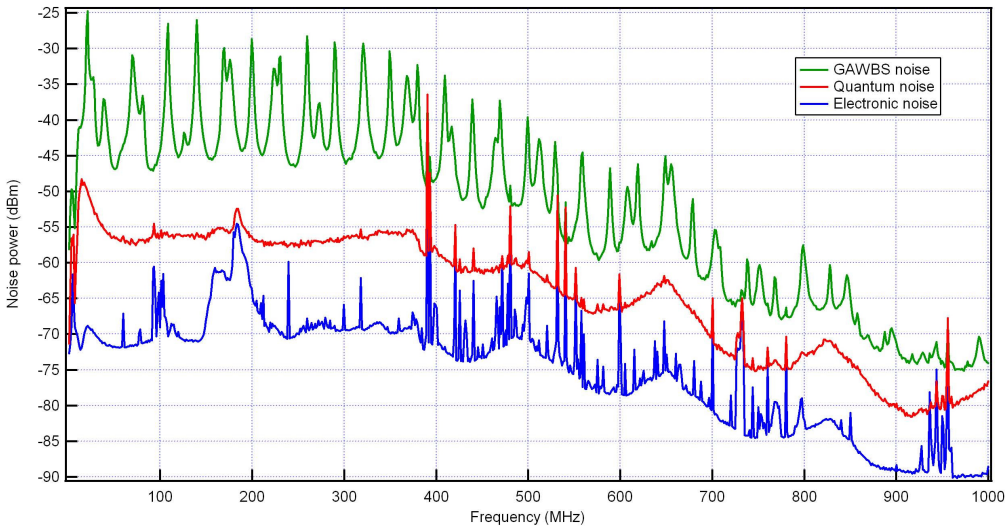


Figure 22: GAWBS noise spectrum measurement. The green line is the GAWBS noise when both the signal and the LO are connect. The red line is the shot-noise limit when only the LO is connect. The blue line is the electronic noise floor obtained by turning off both the signal and the LO.

At the receiver, after 24.2 km of fiber, the LO power is about -6 dBm. Bob separates the LO and the signal by means of PBS2, where the lengths of the LO and the signal paths before recombining are matched to less than 1 mm. As a result of imperfections in the PBS, about 0.07% of the LO leaks into the signal path. The small amount of leaked LO contains detectable GAWBS noise having frequency components up to 1.8 GHz, but the frequency shifted signal remains uncontaminated as it lies beyond the GAWBS spectrum of the CWLO. The signal spectrum now corresponds to Figure 21 (bottom). We now describe how the LO is made to match the signal spectrum. At PBS2, 99.93% of the LO enters the LO path, passing through PM3 which is modulated in the same way as PM1, ideally shifting all of the LO to sidebands, as in Figure 21 (top). Subsequently PM4 performs Bob's random selection of phase. An optical amplifier increases the power of the LO to 15.0 dBm, a 0.8 nm

optical bandpass filter removes amplified spontaneous emission and the LO passes through a polarizer. The signal and LO are mixed on a 50/50 fiber beam splitter (49.8/50.2 in practice) and guided to two photodiodes (Epitaxx ETX75) having a 1.1 GHz 3-dB bandwidth. Because the diodes have no frequency response beyond 1.4 GHz, the different optical sidebands do not beat with each other. Because of the phase coherence of the multi-frequency LO, a single optical mode is measured. A filter follows each photodiode, separating frequencies less than 5 MHz from those greater than 5 MHz. Each photocurrent then enters a 180 degree hybrid bridge (Anzac H-9) producing an RF difference photocurrent. The difference photocurrent passes through a 25 MHz highpass filter, a 50 dB-gain electrical amplifier with noise figure 0.9 dB, then a mixer that brings the 50 MHz RF frequencies to the base band. The down converted photocurrent is finally filtered by a 1.9 MHz filter for A/D sampling. The system is controlled by a computer which uses a training frame to perform real-time adjustment of the phase drift between the signal and LO by addition of a constant to Bob's phase input to PM4. The computer also performs data post selection and classical data correction. A picture of the running experiment in the laboratory is shown in Figure 24.

The detection setup realizes between 64 and 65 dB of common mode noise suppression during experimental runs. This balancing, reached by inducing small loss on one optical fiber and electrical path matching, is sufficient to suppress excess noise that is due to laser RIN noise (7 dB excess noise), GAWBS noise on the LO (15 dB excess noise), and the EDFA (10 dB excess noise). The balancing is checked by the experimental setup shown in Figure 25.

The light from the CW laser is fed to a polarizer then an amplitude modulator driven by a 50 MHz function generator, which creates sidebands 50 MHz apart from the center frequency. The modulated light is amplified by an optical amplifier and filtered by an optical bandpass filter with 0.8 nm linewidth. The filtered light impinges

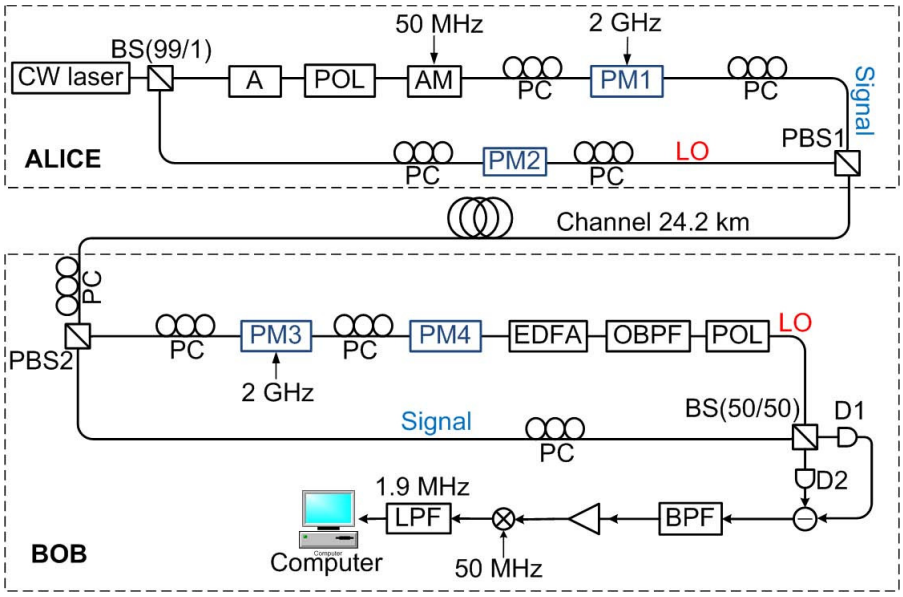


Figure 23: A schematic diagram of the experiment.

on a 50/50 beamsplitter whose two outputs are detected by two photon detectors. A hybrid bridge performs either a sum or a difference operation on the produced photocurrent before injecting the photocurrent to a bandpass filter, and an electronic amplifier with 60 dB gain. An electronic spectrum analyzer is used to measure the spectrum of the photocurrent. By comparing the spectral power density at 50 MHz for the sum photocurrent and the difference photocurrent, the balancing of the homodyne measurement can be measured.

The shot-noise level is also checked by injecting different optical powers to the optical amplifier. The noise power vs EDFA input is shown in Figure 26. The measured noise level approaches a constant for input powers greater than -5 dBm. We believe that for the 50 MHz sideband and -5.6 dBm input power to the EDFA used in the experiment, the homodyne measurement achieves the shot-noise limit.

The overall quantum efficiency is 0.56, with PBS efficiency 0.795, fiber beamsplitter efficiency 0.98, photodiode efficiency 0.74, and effective transmission losses 0.02 that is due to imperfect fiber beamsplitter ratio. During experiments, 7 mW of LO

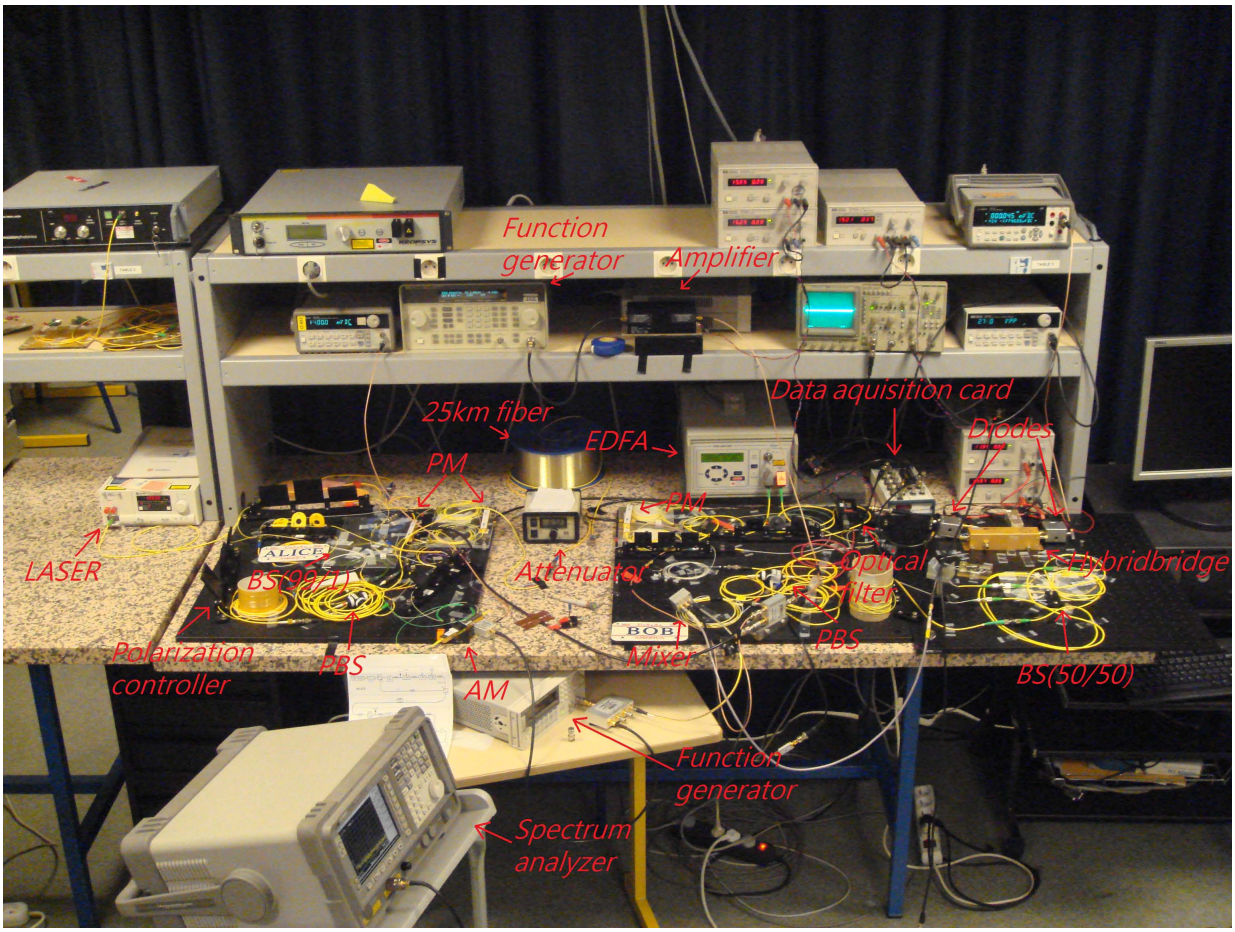


Figure 24: The running experiment in the laboratory. Devices are marked in red font.

power impinges on each detector. At this power level the electric noise is 0.069 shot-noise units. Even when no quantum signal is present, residual excess noise present remains only when Bob's signal path is connected. This noise is believed to be Raman or residual GAWBS noise and results in 0.002 to 0.005 shot-noise units of excess noise remaining at the receiver. We hypothesize that the frequency translation scheme is imperfect due to uncertainty in polarization, modulation voltage, and possibly due to modulator waveguide imperfections. By comparing this to the excess noise present when the 2 GHz RF signal is turned off and 1.0 extra shot-noise unit of GAWBS noise is measured, we estimate 27 dB of GAWBS noise suppression. When the length of the channel is 0 km, no excess noise is present whether the 2 GHz RF signal is

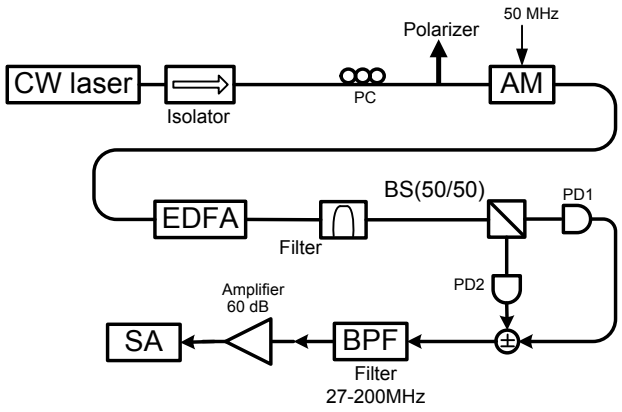


Figure 25: The experimental setup to check the balancing of the homodyne measurements.

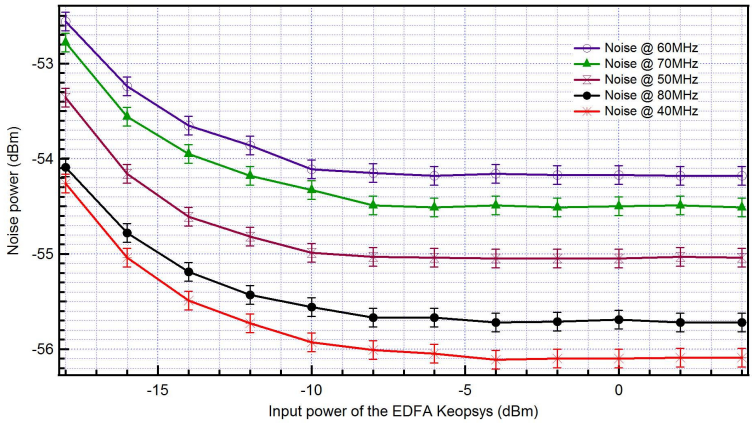


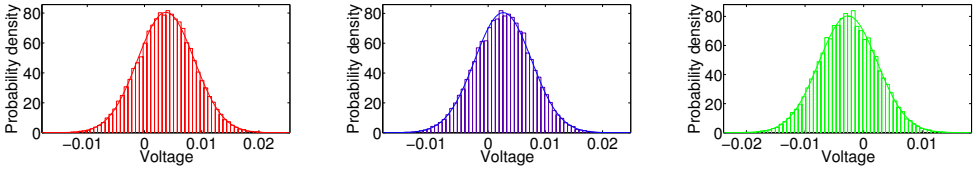
Figure 26: Noise level vs input power to the EDFA measured for different sidebands.

turned off or left on.

3.2.2 Experimental results and discussions

For a 24.2 km channel, a received signal-to-noise ratio of 0.272 (ratio of the signal power to the variance of the shot noise) and post-selection threshold $T = 1.0588$ shot-noise units meet the requirements of the error correction code used in reconciliation. Because in principle Eve could replace the communications channel with a GAWBS-free channel, adding a controlled noise-like source, the excess noise is assumed to be under the control of Eve. According to the protocol, conditional tomography

for all four states has been performed. The results show that the average excess noise of the quantum channel at the detector is 0.0024 shot-noise units, of which 0.0024 is due to GAWBS noise and any remaining imperfections due to the phase estimation, amplitude modulation, and phase modulation are small and difficult to measure. In Figure 27 the raw homodyne tomography histograms are shown for 10^5 samples per phase, which show excellent agreement with the expected Gaussian distribution for coherent light with very small excess noise. Since we have finite amount of tomography data, in a more rigorous security treatment, finite-size effects need to be considered [80]. For each of the four signal states transmitted by Alice, three angles used by Bob's tomography.



(a) Histograms for phase $\frac{1}{4}\pi$ (b) Histograms for phase 0 (c) Histograms for phase $\frac{1}{2}\pi$

Figure 27: Tomography data with Gaussian fit

Given the channel transmission, detection quantum efficiency, excess noise, the post-selection threshold, and the efficiency of the error-correction code (efficiency 80%, error rate 7%), we operate in a secure region [81], obtaining a final key rate of 3.45 kbit/s. A necessary approximation in our security calculation truncates the Fock space to photon number 3, i.e., EMAX in [81] is set to 3. The error in this approximation is negligible, as setting EMAX = 2 gives a secret-key capacity that differs from EMAX = 3 by only 10^{-7} bit/channel use. We note that unlike previous experiments [45], this experiment is not constrained by the time required for the error correction code, but by the data rate, which is limited by the 2 MSa/s data acquisition and control card (National Instruments PCI-6115). We have not implemented automatic polarization control at the input of Bob's PBS2, so the system operates well for 7 minutes before the polarization needs to be readjusted. The same

experiment operating at a 20 MHz clock rate would leave us with a final key rate of approximately 60 kbit/s with our current error-correction code. Therefore, our implementation loosens the requirement on the efficiency of error-correction codes and possesses potential to increase the key-generation rates to an order of magnitude higher than current CVQKD systems.

3.2.3 GAWBS noise tomography

The statistical distribution of the GAWBS noise is important for security analysis. In Sec. 3.1.2, we assumed that the statistical distribution of additional noise, which is mostly GAWBS noise in a real experiment, is Gaussian. To validate this assumption, we need to make experimental measurements on the GAWBS noise and show its statistical distribution. The experimental method we adopt here is quantum tomography in which we measure the quadrature distribution of the incoming signal containing GAWBS noise with a strong local oscillator.

When a strong local oscillator and weak signal are polarization multiplexed, several optical processes can potentially produce noise due to scattering from the local oscillator to the signal band. These processes include four-wave mixing, spontaneous Raman scattering, and GAWBS noise. We examine each in turn in order to ascertain its contribution.

We examine four-wave mixing first. We first check to see if the four-wave-mixing interaction is approximately phase matched. We calculate the accumulated phase mismatch to be $\Delta kL = \beta_2(2\pi f)^2 L$, where $L = 24$ km is the fiber length, Δk is the phase mismatch, β_2 is the dispersion of the fiber, and f is the frequency detuning in Hertz between the LO and the signal beam. To have an accumulated phase mismatch of less than π radians at frequency f, we require $f \leq (4\pi|\beta_2|L)^{-1/2} \approx 22$ GHz for our SMF fiber with dispersion 17 ps nm^{-1} km^{-1}. As the frequencies in the experiment are less than 10 GHz, four-wave mixing will need to be considered. One can make a precise

calculation of the number of spontaneously emitted photons from [82]. However, a conceptually simple upper limit can be found by estimating the mean number of four-wave mixing photons emitted per mode as

$$\bar{n} \leq (\gamma P L_{\text{eff}})^2, \tag{3.2.1}$$

where the effective length of the 24.2 km optical fiber for four-wave mixing is $L_{\text{eff}} = (1 - \exp(-\alpha L))/\alpha = 14.1$ km and $\alpha = 0.0495$ km^{-1} corresponding to 0.21 dB loss per km. The nonlinear coefficient γ is estimated to be 0.33 W^{-1} km^{-1} for cross-polarized four-wave mixing in SMF [83]. This gives a mean photon number per mode of $\bar{n} = 2 \times 10^{-5}$ for 1 mW of input, the input level in [84] and $\bar{n} = 2 \times 10^{-3}$ for 10 mW of input, the upper limit of LO power used in this tomographic measurement.

We next evaluate the spontaneous emission of Raman photons. An appropriate formula for the modal mean number of spontaneously emitted Raman photons in the limit of small detuning is

$$\bar{n}_{\text{Raman}} = R_g'(0)(kT/h)L_{\text{eff}}P, \tag{3.2.2}$$

which is derived by taking the limit of Eq. 1 or Eq. 2 in [42] as the detuning of the Raman pump approaches zero. For SMF, we estimate that the slope of cross-polarized Raman gain spectrum in SMF is 0.01×10^{-12} W^{-1} km^{-1} Hz^{-1}, using a gain half that of the experimental value in DSF fiber in [83]. This gives a resulting $\bar{n}_{\text{Raman}} = 8.8 \times 10^{-4}$ for 1 mW of LO power and $\bar{n}_{\text{Raman}} = 1.6 \times 10^{-3}$ for 10 mW of LO power.

GAWBS [79] is a linear process that can produce unwanted noise in both pulsed and continuous wave (CW) quantum optics and quantum communications experiments [85, 86]. As light propagates along an optical waveguide, thermally populated acoustic waves having frequencies up to roughly 2.0 GHz produce waveguide density fluctuations, which in turn scatter light both in a forward and backward direction. GAWBS usually refers to the forward scattered light with co-polarized and

un-polarized components coming from radial acoustic waves and mixed torsional-radial acoustic waves respectively [87]. Of particular interest in this paper is the part of the un-polarized component scattered into the polarization orthogonal to the LO.

Our CVQKD experiment [84] measured additive noise in shot-noise units, where 1 shot-noise unit is experimentally the photocurrent variance of homodyne measurements minus the variance of electronic noise with no input. Thus, one shot-noise unit is equivalent to 1/2 of a photon. The measurements in [84] resulted in a minimum excess noise of 0.002 shot-noise units, so we estimate the total number of excess noise photons produced in the fiber to be the excess noise in shot-noise units divided by two and also by the quantum efficiency. This means that the excess noise measured in the experiment corresponded to approximately 0.004 photons. Thus we conclude that Raman scattering accounted for at most one-fourth of the excess noise measured in the QKD experiment and the contribution of four-wave mixing was negligible.

The remaining noise comes from from GAWBS scattering and also potentially from classical imperfections in the control of LO phase. Evidence that GAWBS scattering dominated was the fact that a GAWBS noise reduction scheme reduced excess noise [84].

Our experimental setup measures cross-polarized GAWBS noise. The schematic of the experimental setup is shown in Figure 28. Alice transmits a CWLO through 24 km fiber, where both polarized and depolarized GAWBS noise will be created in the sidebands of the CWLO. In order to obtain strong GAWBS signals to better characterize it, 10 mW of LO power is injected. After traveling through the fiber, the LO and cross-polarized noise are separated by a polarizing beamsplitter.

The detection scheme is motivated by the following considerations: first, the balanced detector has its best performance when measuring 50 MHz RF offsets from the optical LO. This is due to the hybrid bridge used in the balanced detection circuit. Second, we wish to measure GAWBS noise at offsets greater than the bandwidth of

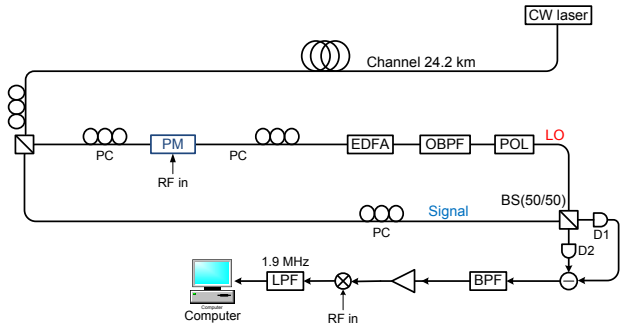


Figure 28: GAWBS measurement setup.

the detectors (1100 MHz). In order to accomplish this, we drive the phase modulator (PM) with a driving voltage chosen so that the modulator phase shift amplitude corresponds to the first root of the Bessel function J_0. The result is that the LO light is frequency shifted away from its original frequency into several sidebands. The LO thus samples a superposition of frequencies displaced by multiples of f_{PM}. The measured difference photocurrent is down converted to the base band by mixing with an RF LO at frequency f_{RFLO}, where f_{RFLO} is either 45, 50, or 55 MHz, thus achieving excellent balancing.

At the receiver, after 24 km, for which the linear loss is about 5 dB, the LO power is about 5 dBm. The polarization beam splitter (PBS) separates the strong CWLO and the GAWBS that is on the orthogonal polarization than the LO. The strong LO goes into LO path and the scattered GAWBS goes into the signal path. Due to the imperfection of the PBS, there is about 0.07% of LO power leaked into the signal path. At the LO port 99.93% of the LO enters the LO path, passing through a PM. The LO is entirely frequency shifted away from the optical LO frequency creating several sidebands spaced f_{PM}. The LO spectrum and signal spectrum in front of the homodyne detection device are represented schematically in Figure 29(a) and Figure

29(b), respectively.

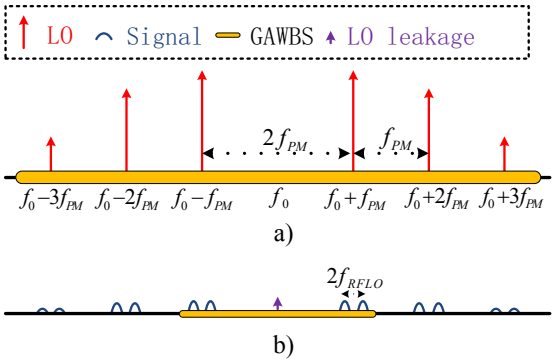


Figure 29: Spectrum of a) LO before balanced detection, schematically representing co-polarized GAWBS noise in yellow and b) schematic of the spectrum of cross-polarized GAWBS noise, the detected frequencies are schematically represented by blue raised curves having centers located $\pm f_{\mathrm{RFLO}}$ from each LO component.

The LO and the signal are mixed on a 50/50 fiber beam splitter (49/51 in practice) and guided to two photodiodes (Epitaxx ETX75) having a 1.1 GHz 3-dB bandwidth. The LO that specifies the single mode that undergoes quantum homodyne detection thus corresponds to a sequence of several optical frequencies separated by f_{RFLO} , but having no component at the center frequency, that of the LO laser. A filter follows each photodiode, separating frequencies less than 5 MHz from those greater than 5 MHz. Each photocurrent then enters a 180 degree hybrid bridge (Anzac H-9), producing an RF difference photocurrent. The photocurrent passes through a 25 MHz highpass filter, a 50 dB electrical amplifier with noise figure 0.7 dB, and a mixer with input from a function generator to bring the f_{RFLO} sideband signal to the base band. f_{RFLO} takes on values of either 45 MHz, 50 MHz, or 55 MHz in this experiment. The output is then finally filtered by a 1.9 MHz filter for A/D sampling. A computer performs data acquisition. The detection setup realizes between 55 and 62 dB of common mode noise suppression during experimental runs. This balancing, reached by inducing small loss on one optical fiber and electrical path matching, is sufficient

to suppress excess noise due to laser RIN noise (7 dB excess noise), GAWBS (15 dB excess noise), and EDFA (10 dB excess noise). The overall quantum efficiency is 0.54, with PBS efficiency 0.795, fiber beamsplitter efficiency of 0.98, photodiode efficiency 0.74, and effective transmission losses of 0.02 due to imperfect fiber beamsplitter ratio. During experiments, 7 mW of LO power impinges on each detector. At this power level the electric noise is 0.085 shot-noise units.

The driving signal frequency of the PM was tuned from 950 MHz to 2000 MHz and the noise power measured. Because the GAWBS noise spectrum is essentially absent above 1900 MHz, the portion of the LO present at harmonics of the PM frequency sample vacuum, or extremely weak Raman scattering, to be more precise. The mean number of measured photons in a 1.9 MHz bandwidth vs. driving signal frequency of the PM is shown in Figure 30, which results in a typical GAWBS spectrum. The calibration of vacuum input is used for calibration. The GAWBS peaks are spaced roughly 50 MHz apart, and become very small above 1750 MHz, and zero at 2000 MHz. The measured GAWBS noise is with sensitivity of approximately 0.01 shot-noise units. Because the mode measured contains two pairs of sidebands, each pair approximately 100 MHz apart, a GAWBS peak in Figure 30 should be considered to be a superposition of GAWBS noise at $\pm f_{\mathrm{PM}} \pm f_{\mathrm{RFLO}}$. Each peak in the spectrum corresponds to a guided acoustic wave mode in the optical fiber. One would expect that each scattering event that occurs in the optical fiber results in a photon whose phase is uncorrelated with the phase of the LO beam. By the law of large numbers, the field statistics should become Gaussian and equivalently, the photon statistics should become Bose-Einstein (also called thermal). In Figure 31, we show phase-averaged quantum statistics for several of the measured frequencies on a semi-log scale. The homodyne statistics are shown to be Gaussian to up to 55 dB of dynamic range. We next feed our experimental data to the chi-square goodness-of-fit statistical test. The test results are listed in Table 1. The test shows extremely strong agreement with

the expected statistics for all driving frequencies of the phase modulator and signal side-band frequencies. A total of 11.9 M samples were obtained for each curve. From the figure, we can conclude that the noise distribution of the noise is very Gaussian, for which our default secret-key capacity calculation model in [81] is suitable.

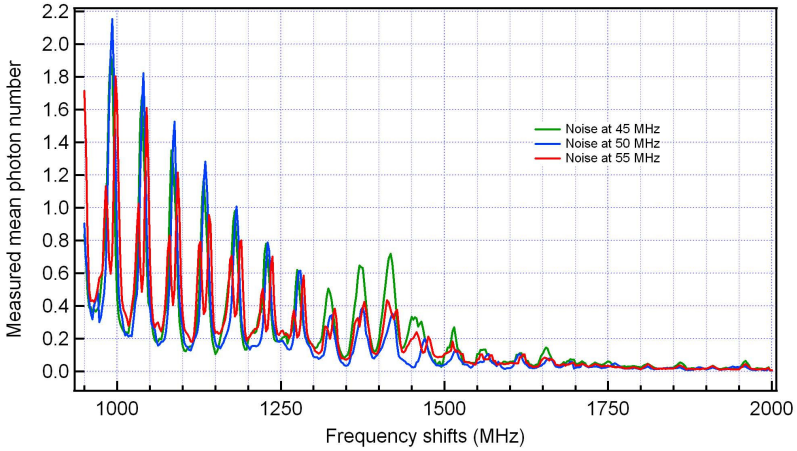


Figure 30: Cross-Polarized GAWBS spectrum scattered from a 10 mW LO injected in 24.2 km SMF fiber. Green curve, $f_{\mathbf{RFLO}} = 45$ MHz; Blue curve, $f_{\mathbf{RFLO}} = 45$ MHz; Red curve, $f_{\mathbf{RFLO}} = 45$ MHz.

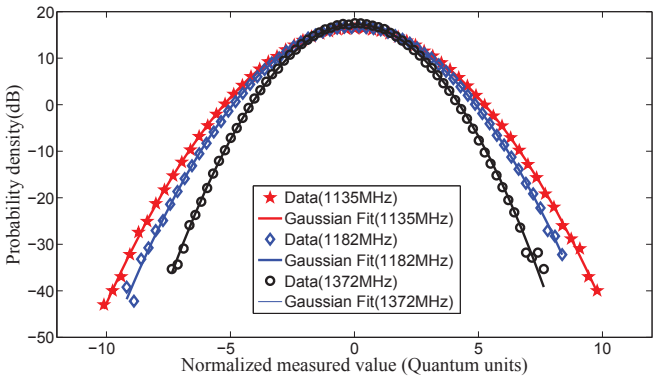


Figure 31: Homodyne statistics on a semi-log scale. Normalized probability density vs. homodyne measurements in quantum units.

Table 1: Chi-square goodness-of-fit statistical test. $f_{\mathbf{PM}}$ is the driving frequency to the phase modulator, and $f_{\mathbf{S}}$ is the side-band detection frequency in the homodyne measurement. If $h = 0$, the null hypothesis that the experimental data are a random sample from a normal distribution with mean and variance estimated from the experimental data cannot be rejected at the 5% significance level.

Frequencies	h	p-value
f_{PM}= 1132 MHz, f_{S}= 45 MHz	0	0.3428
f_{PM}= 1180 MHz, f_{S}= 45 MHz	0	0.16
f_{PM}= 1170 MHz, f_{S}= 45 MHz	0	0.4405
f_{PM}= 1135 MHz, f_{S}= 50 MHz	0	0.2057
f_{PM}= 1182 MHz, f_{S} = 50 MHz	0	0.1849
f_{PM}= 1372 MHz, f_{S} = 50 MHz	0	0.1218
f_{PM}= 1140 MHz, f_{S}= 55 MHz	0	0.1340
f_{PM}= 1190 MHz, f_{S}= 55 MHz	0	0.9193
f_{PM}= 1380 MHz, f_{S}= 55 MHz	0	0.7276

CHAPTER IV

QUANTUM RANDOM-NUMBER GENERATION

Quantum key distribution (QKD) allows the accumulation of key bits that are perfectly secure if protocols are correctly implemented and side-channel attacks can be ruled out. The key material can be used as a key for a one-time pad, which maintains perfect security but uses one key bit per encrypted message bit. On the other hand, however, the security of QKD implementation is influenced by the random numbers that are used to choose Alice and Bob's encoding and decoding basis. Use of pseudo-random numbers is not allowed in QKD because an eavesdropper with unlimited computational power can in principle make an exhaustive search to break the algorithm used to produce pseudo-random numbers and thus achieve perfect correlation with Bob's quantum measurements. Therefore, QKD requires true-random numbers that can neither be predicted nor be reproduced. True-random numbers also have significance in classical cryptography. They are necessary elements to construct random mathematical problems, to be sent as authentication challenges, to generate prime numbers, and to generate passwords. A large amount of true-random numbers are also required in Monte-Carlo simulations, in spectrum spreading telecommunication systems, and in gambling industry.

In this chapter, we introduce a quantum random-number generator based on amplified spontaneous emission (ASE). Compared to existing physical random generators, the proposed quantum random-number generator possesses advantages including true randomness, large bandwidth, and easy implementation. We will first describe the experimental implementation of the quantum random-number generator based on ASE, and later theoretically study its performance and limits.

4.1 The experimental implementation

Amplified spontaneous emission (ASE) is a quantum mechanical phenomenon that can be used to generate randomness. Compared to classical pseudo-random-number generation, the ASE possesses the benefit of true randomness and ultrahigh bandwidth. We use ASE light at 1550 nm as our quantum random-number source, a convenient source that yields experimental statistics predicted by quantum models. The basic experimental setup is described in Figure 32.

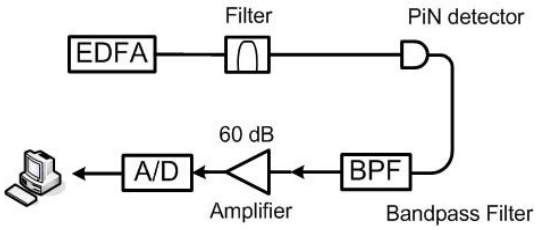
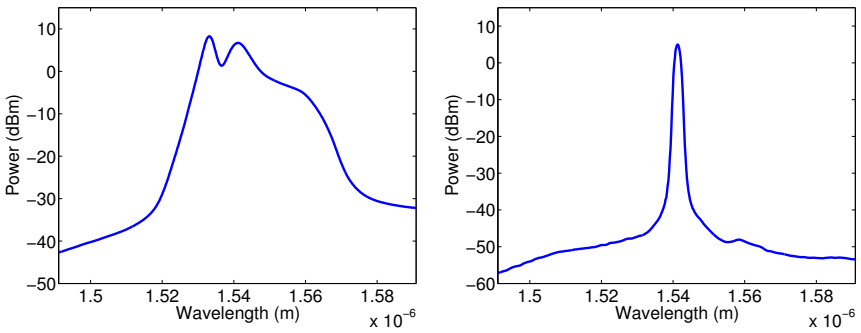


Figure 32: The experimental schematic of the quantum random-number generator based on ASE.

The light is emitted from an ASE source, an erbium-doped fiber amplifier (EDFA). EDFA produces high-power, large-bandwidth ASE light. In practice, light-emitting diode (LED) is more suitable for practical use with lower cost than EDFA. The emitted light is either filtered by an 0.8 nm optical bandpass filter then injected into an optical spectrum analyzer (OSA) or injected directly into an OSA. The obtained spectra from the OSA are shown in Figure 33.

The filtered ASE light is fed to a photodiode with a 2 GHz bandwidth. Since the detector bandwidth is larger than the ASE light bandwidth, multi-mode measurements are performed. For a single-mode measurement on ASE light, the photocurrent is Bose-Einstein distributed. However, multi-mode measurement yields a degenerate Bose-Einstein distribution [88]. As the ratio of the ASE light bandwidth to the detector bandwidth, defined as the degeneracy, becomes large, the degenerate Bose-Einstein distribution converges to a Gaussian distribution. The acquired photocurrent is then fed to an electronic bandpass filter with bandwidth from 41 MHz to 2



(a) The optical spectrum of the ASE light directly from the EDFA.

(b) The optical spectrum of the filtered ASE light by a 0.8 nm optical bandpass filter.

Figure 33: The ASE optical spectra. The EDFA output power is 18.5 dBm. The insertion loss of the optical bandpass filter is measured to be 3 dB.

GHz. The output from the bandpass filter is amplified by an electronic amplifier with 1.5 GHz bandwidth 60 dB gain. The electronic spectra of the amplified photocurrent and the pure electronic noise are shown in Figure 34. Since the photocurrent power is

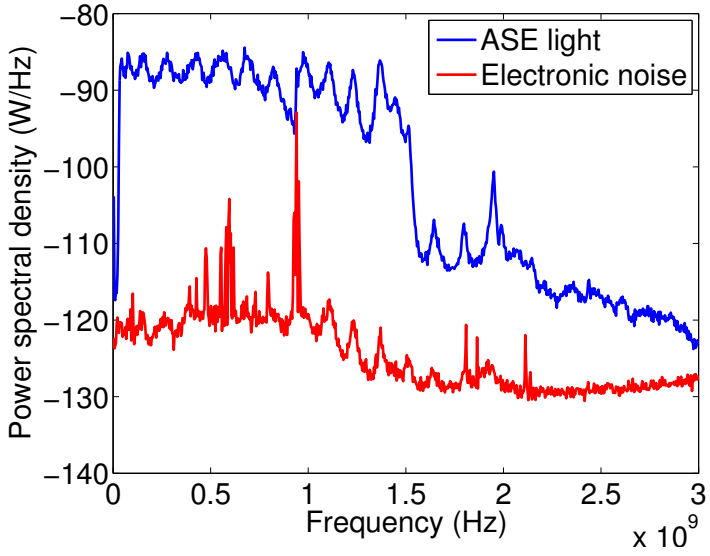


Figure 34: The power spectral density of the ASE light and the electronic noise.

30 dB above the electronic noise floor, the quantum noise dominates the signal. The amplified photocurrent is sampled by a high-rate oscilloscope with 8-bit resolution. A sampled digital data is shown in Figure 35. In Figure 36, we try to fit a sampled digital data to a Gaussian distribution. The sampled digital data is then differentiated

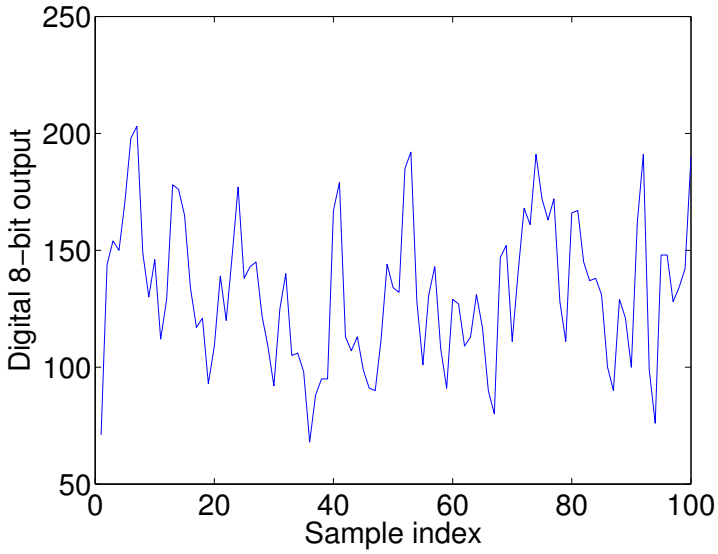


Figure 35: A sampled digital data in the time domain. The EDFA output power is 18.5 dBm, the total loss is 8.5 dB, and the sampling rate is 4 GHz.

to remove offset, i.e., the difference between two consecutive samples is recorded.

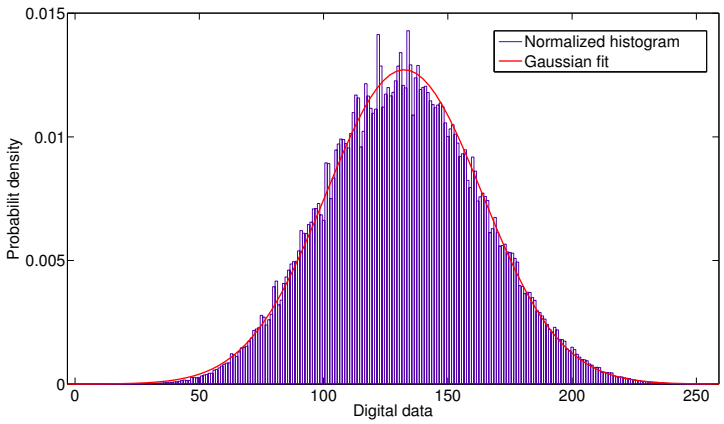


Figure 36: A Gaussian fit to the sampled digital signal, the EDFA output power is 18.5 dBm, total loss is 10 dB, and the sampling rate is 4 GHz.

We operate in a region where the sampling rate equals to the bandwidth of the signal. As we will see, the correlation coefficient of quantized random binary sequences is negligible. We acquired 1000 random bit blocks with 100000 kbits in one block. We then feed the acquired random bits into the NIST randomness tests. For a 4 GHz sampling rate, the first 5 least significant bits of the 8-bit quantized digital

data passed all NIST randomness tests (Table 2). This implies a random-number generation rate at 20 Gbit/s. The produced random numbers can be compressed by a hash function, which can remove possible pseudo-randomness from the electronic noise.

Table 2: The NIST random-number-tests results.

bit	**Result**
LSB	Pass
LSB + 1	Pass
LSB + 2	Pass
LSB + 3	Pass
LSB + 4	Pass
MSB - 2	Fail
MSB - 1	Fail
MSB	Fail

We also take another set of data from a different hardware setup. We remove the bandpass filter in our original setup and acquire 448 M samples with 4 GSa/s acquisition rate. We first make a differential operation on the original acquired samples. We then separate bits from different levels. By doing this, we generate eight binary files containing bits from the least significant bit to the most significant bit of each differentiated sample. We then feed the eight files separately to the NIST random-number tests. The result shows that the first four least significant bits pass the NIST tests. Compared to the result we get before, the fifth least significant bit does not pass the tests. This is because once the bandpass filter is removed, some deterministic periodic patterns decrease the randomness in our samples. We also perform a cross-level random-number test. We take four least significant bits, which pass the NIST tests individually, from each sample and catenate them to form a big binary file. The structure of the a binary test sequence is illustrated in Figure 37. The size of each binary test sequence is 10 M bits, and we use 100 binary sequences for the NIST tests. As a result, the total number of bits tested by the NIST tests is

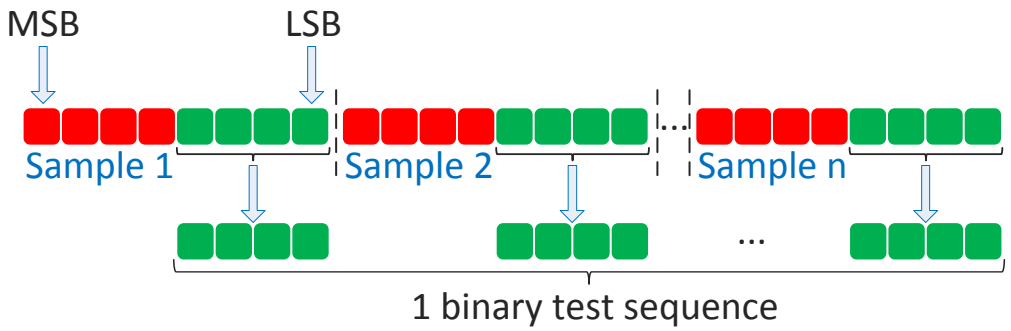


Figure 37: The structure of a binary test sequence.

1 G. These binary sequences pass the NIST tests. Thus, we conclude that there are no significant cross-level correlations.

4.2 Performance analysis

4.2.1 The probability distribution of the photocurrent

Photons from ASE light are Bose-Einstein distributed. Let the average photon number in one mode be $\bar{n}$. For a single-mode measurement in which the detector coincides with the ASE light bandwidth, the probability to find m photon reads [88]

$$p_S(m) = \frac{\bar{n}^m}{(1+\bar{n})^{1+m}}. \tag{4.2.1}$$

Since the bandwidth of the filtered ASE light is much greater than the photon detector bandwidth, multi-mode measurements with degeneracy g are performed. The photon probability distribution is a g-fold-degenerate Bose-Einstein distribution

$$p_M(m) = \frac{\Gamma(m+g)}{\Gamma(m+1)\Gamma(g)} \left(1+\frac{1}{\bar{n}}\right)^{-m} (1+\bar{n})^{-g}, \tag{4.2.2}$$

resulting from a g-time convolution of Eq. 4.2.1. The degeneracy g can be found by

$$g = 2 \times \frac{B_A}{B_D}, \tag{4.2.3}$$

where B_A and B_D are the ASE bandwidth and the detector bandwidth respectively. The coefficient 2 is due to polarization degeneracy. With $g \gg 1$, the photon statistics

converge to Gaussian. In our experimental implementation, the filtered ASE bandwidth is 100 GHz, giving $g = 133$. To verify the photon statistics, we fit the sampled digital data to either Gaussian statistics or degenerate Bose-Einstein statistics and plot the fits on semi-log scales in Figure 38. The fit returns $g \approx 110$, showing agree-

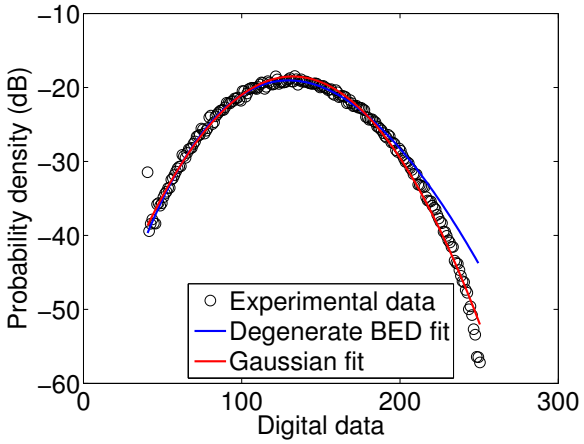


Figure 38: The statistical fit of the sampled signal.

ment with our degeneracy estimate. Degenerate Bose-Einstein statistics certainly give a better fit over the whole range except for the most right areas. We ascribe this divergence to the integral nonlinearity of our A/D converter. The dynamic ranges are limited by the resolution as well as the memory depth of the oscilloscope.

4.2.2 Bit correlation

We next analyze the autocorrelation of the acquired data. Let the random signal be $X(t)$, with the time-varying mean $\mu(t)$ and variance $\sigma(t)$. The autocorrelation of $X(t)$ is defined as

$$R(t_1, t_2) = \frac{E\left[(X(t_1) - \mu(t_1))(X(t_2) - \mu(t_2)\right]}{\sigma(t_1)\sigma(t_2)}. \tag{4.2.4}$$

The mean $\mu(t)$ and the variance $\sigma(t)$ are time dependent in general. However, for the wide-sense stationary process, we have the time-independent mean

$$E[X(t)] = \mu(t) = \mu(t + \tau), \tag{4.2.5}$$

and the autocorrelation

$$R(t_1, t_2) = R(t_1 - t_2, 0) \equiv R(\tau) \tag{4.2.6}$$

only depends on the time interval $\tau = t_1 - t_2$. Once the autocorrelation of a wide-sense stationary process is given, its power spectral density can be obtained by the Fourier transform

$$S(f) = \int_{-\infty}^{\infty} R(\tau) e^{-2\pi i f \tau} d\tau, \tag{4.2.7}$$

which is known as the Wiener-Khinchin theorem. Conversely, given the power spectral density of a wide-sense stationary process, its autocorrelation can be derived by the inverse Fourier transform

$$R(\tau) = \int_{-\infty}^{\infty} S(f) e^{2\pi i f \tau} df. \tag{4.2.8}$$

Let the electric field of the filtered ASE light be

$$E(t) = A(t) e^{i[\theta(t) + \omega t]} + \text{c.c.}, \tag{4.2.9}$$

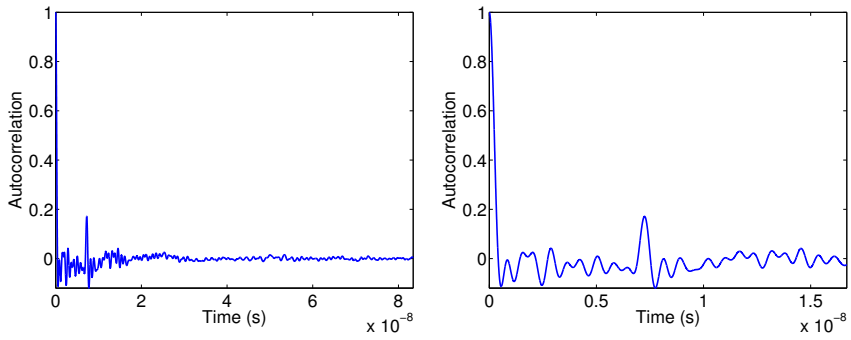
where $A(t)$ is the time-varying amplitude envelope and $\theta(t)$ is the time-varying phase. The photocurrent produced by the photo detector is proportional to the electric field intensity:

$$i(t) \propto |E(t)|^2 = |A(t)|^2. \tag{4.2.10}$$

The power spectral density of $i(t)$ is defined as

$$S_i(f) = E\left[\lim_{T \to \infty} \frac{1}{T} \left| \int_{-T/2}^{T/2} i(t) e^{-2\pi i f t} dt \right|^2 \right]. \tag{4.2.11}$$

Once the power spectral density of the photocurrent is obtained, we can evaluate its autocorrelation by performing an inverse Fourier transform. Experimentally, we obtain the power spectral density of the photocurrent from an electronic spectrum analyzer. To calculate the autocorrelation, we use the electronic spectrum in Figure 34, and perform a inverse Fourier transform. The result is shown in Figure 39.



(a) The autocorrelation of the photocurrent.

(b) The autocorrelation of the photocurrent. Only the first 15 ns are plotted.

Figure 39: The autocorrelation of the amplified photocurrent. The autocorrelation is calculated from the electronic spectrum plotted in Figure 34 .

The autocorrelation exhibits a dramatic drop at about 0.5 ns, coinciding with the electronic bandpass filter bandwidth.

We next evaluate the autocorrelation of individual quantized bits produced by the oscilloscope. In Figure 40, we plot the autocorrelations for the least significant bit (LSB), the second most significant bit (MSB-1), and the most significant bit (MSB). We find that the autocorrelation for the LSB is 0 while there exist strong autocor-

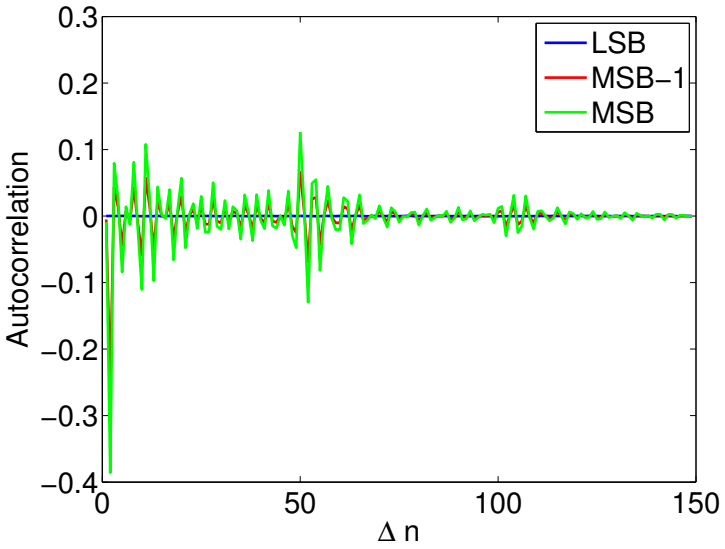


Figure 40: The autocorrelations of individual bits. The plot spans the range from $R(1)$ to $R(150)$.

relations for the second MSB and the MSB, which results from residual correlation between two successive samples. True randomness is contained in the least significant bits. The NIST random number tests give some confidence that the first five LSBs are random.

To analyze the correlation across different quantization levels, e.g., the LSB and the LSB-1, we calculate the cross-correlation of these bits. We plot the cross-correlation between the LSB and the LSB-1 in Figure 41. The average absolute value of the cross-correlation is 1.35×10^{-4}. Compared to the average absolute value 1.49×10^{-4} of the autocorrelation of the LSB, which passes the NIST tests, we conclude that there is no correlation among different quantization levels.

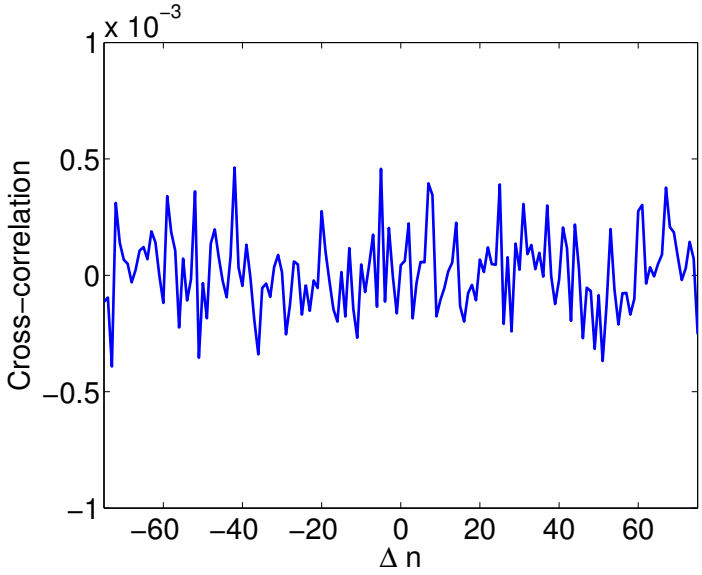


Figure 41: The cross-correlations between LSB and LSB-1.

4.2.3 Performance limits

Although passing standard random tests is a necessary condition for true randomness, it is not sufficient. To guarantee that we do not produce more random bits than the amount of randomness contained in the source, we next investigate the entropy rate of the ASE light, which is also useful information to judge the performance limits of the randomness source.

The photon probability statistics of a multi-mode measurement are degenerate Bose-Einstein distribution. The source entropy in bit can be calculated by

$$H_M = \sum_{n=0}^{\infty} -p_M(n) \log_2[p_M(n)]. \tag{4.2.12}$$

The total entropy rate is the product of the entropy per measurement and the detector bandwidth:

$$R_M = H_M B_D. \tag{4.2.13}$$

In Figure 42, we plot the entropy rate of a multi-mode measurement as a function of the detector bandwidth. Since the EDFA output power is 18.5 dBm, the optical

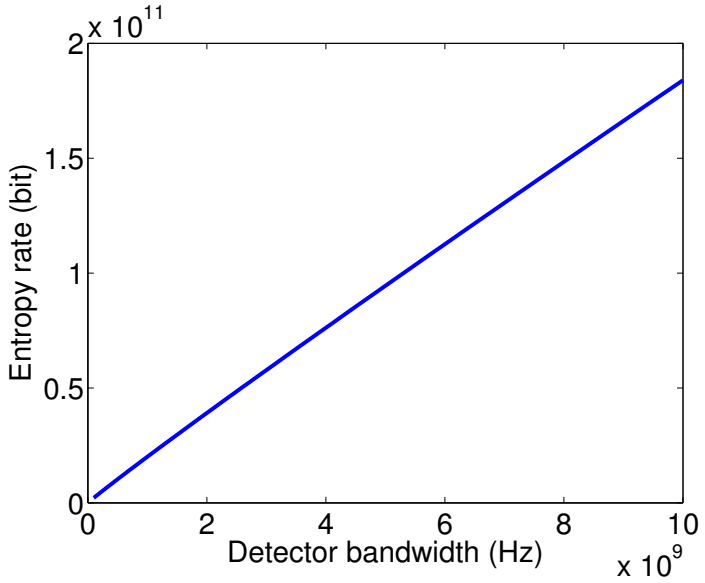


Figure 42: The entropy rate as a function of the detector bandwidth. The EDFA output power is 18.5 dBm, the total loss is 8.5 dBm, the ASE bandwidth is 2 THz, and the optical bandpass filter bandwidth is 100 GHz.

attenuator loss is 5.5 dB, and the insertion loss of the optical filter is 3 dB, the effective ASE power in our experiment is 10 mW. The entropy rate for 2 GHz detector bandwidth is 40 Gbit/s, which is estimated to be the limit randomness production rate with our current setup. The entropy rate is also a function of the ASE power. We plot the entropy rate for a multi-mode measurement as a function of the ASE light power in Figure 43. Figure 43 illustrates that increasing the power of the source is not

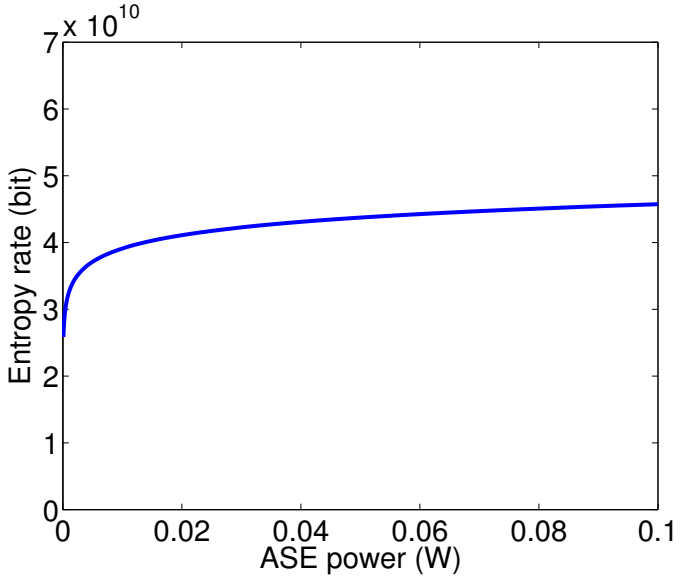


Figure 43: The entropy rate as a function of the ASE light power. The detector bandwidth is set to be 2 GHz. The ASE light bandwidth is 2 THz and the optical bandpass filter bandwidth is 100 GHz.

as an efficient way to increase the entropy rate as increasing the detector bandwidth. The reason is because the entropy of a Gaussian probability distribution only goes logarithmically with its variance, indicating that the entropy in one measurement goes logarithmically with the input power. This explains the logarithmic-like curve in Figure 43.

We next calculate the entropy rate of a single-mode measurement, regarded as a lower bound on the entropy rate of ASE source with photon detection. For a single-mode measurement, $g = 1$. For each measurement, the mean number of photons impinging the photon detector is

$$N_S = \frac{\eta P}{\hbar \omega B_A}. \tag{4.2.14}$$

The entropy per measurement can be calculated by Eq. 4.2.1:

$$H_S = -\sum_{n=0}^{\infty} p_S(n) \log_2[p_S(n)]. \tag{4.2.15}$$

The entropy rate is

$$R_S = 2 H_S B_A, \tag{4.2.16}$$

where the coefficient 2 is included because of polarization degeneracy. In Figure 44, we plot the entropy rate of a single-mode measurement as a function of the ASE light bandwidth. As expected, the entropy rate in a single-mode measurement goes

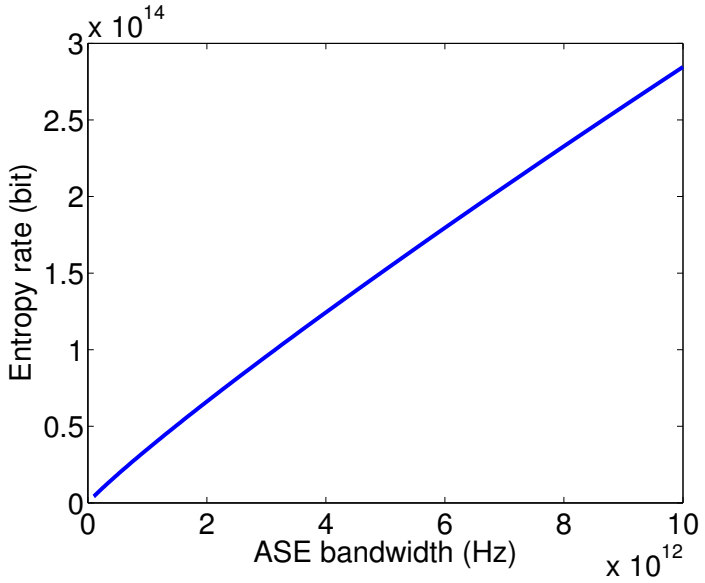


Figure 44: The entropy rate as a function of the ASE light bandwidth in a single-mode measurement. The EDFA output power is 18.5 dBm, the total loss is 8.5 dB, and the optical bandpass filter bandwidth is 100 GHz.

almost linearly with the ASE light bandwidth. For a 2 THz ASE light bandwidth, the ultimate entropy rate reaches 35 Tbit/s. In Figure 45, we plot the entropy rate for single-mode measurement as a function of power. Similarly to the situation in a multi-mode measurement, increasing the ASE light power does not significantly increase the entropy rate. The entropy rate scales logarithmically with the ASE light power.

4.3 Comparison of different random-number sources

For the state of the art, there exist several different physical random-number sources. In this section, we compare three recently implemented physical random-number generators by using chaotic dynamics of a distributed feedback (DFB) laser [26], quantum homodyne measurements [24], and ASE light.

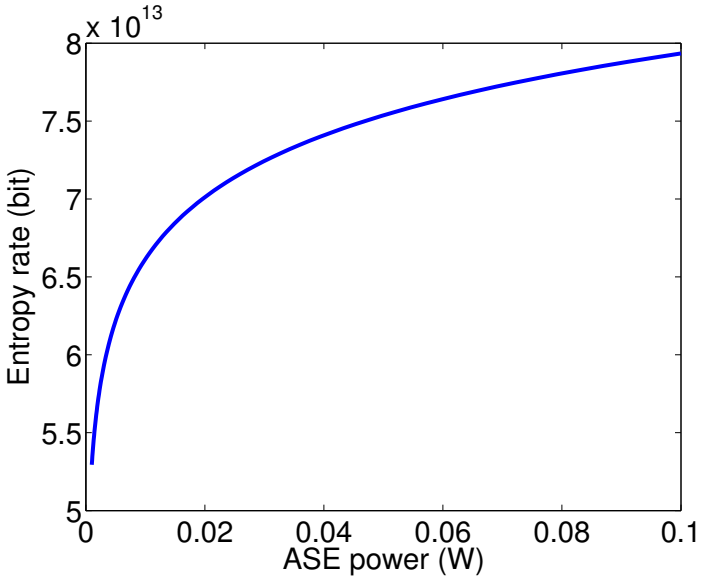


Figure 45: The entropy rate as a function of the ASE light power in a single-mode measurement. The ASE light bandwidth to 2 THz and the optical band-pass filter bandwidth is 100 GHz.

A random-number generator based on chaotic dynamics of a DFB laser was implemented in [26]. The random-number generation rate reached 140 Gbit/s. Due to the physical nature of optical chaos, the dynamics of optical chaos are governed by nonlinear differential equations. These nonlinear differential equations behave very differently depending on their initial conditions. In general, given the solution to a set of nonlinear differential equations, it is mathematically hard to reversely obtain the initial condition. Once additional electronic and other noise are neglected, chaos based random-number generators are pseudo random since their security depends on how hard the nonlinear differential equations can be reversely solved.

In [24], a true random-number generator based on quantum balanced homodyne measurements on vacuum noise was demonstrated. The random-number generation rate reached 6.5 Mbit/s. Since homodyne measurements detect electromagnetic quadratures, the measurement results are continuous random variables with infinite resolution. To perform a quantum balanced homodyne measurement, a strong local oscillator that is aligned to be temporal coherent with the signal to be measured is

required. Furthermore, balanced homodyne measurements also need careful match of both the intensity and the phase of the two arms of the beam splitter to cancel the excess noise from the local oscillator. All these requirements make experimental implementations hard.

In Table 3, we make a comparison of the three physical random-number sources.

Table 3: Comparison of three random-number sources.

Source	**Rate**	**Randomness**	**Resolution**	**Implementation**
Optical chaos [26]	140 Gbit/s	Pseudo	Finite	Simple
Vacuum noise [24]	6.5 Mbit/s	True	Infinite	Hard
ASE	20 Gbit/s	True	Finite	Simple

Recently, we have become aware of a ASE based random-number generator [89] paper appeared in Optics Express after we presented our results in FiO 10 [90]. Reference [89] achieved 12.5 Gbit/s random-number-generation rate by employing two large-bandwidth photodetectors and performing single-mode measurements.

For our future work, we suggest to replace the EDFA by a lower-cost light-emitting diode. We also suggest to model random bits at different quantization levels quantum mechanically.

CHAPTER V

NONLINEAR OPTICS OF GRAPHENE

Earlier in this thesis we demonstrated a state-of-the-art continuous-variable quantum key distribution (CVQKD) system. The CVQKD protocol lies in the network layer of the quantum-communication architecture while the CVQKD experiment and the incidental quantum random-number generator is divided into the data-link layer. We are also interested in the physical layer of the quantum-communication architecture and making contributions to other types of quantum-information systems.

One significant difference between quantum systems and classical systems is that several quantum systems can be entangled. Quantum entanglement is an essential element for quantum teleportation [15], with which we can send quantum states without transmission on the real quantum channel, and thus, the quantum communication distance can be greatly improved to more than 200 km. Quantum entanglement can be produced in nonlinear optical processes such as spontaneous parametric down conversion and four-wave mixing. Current quantum entanglement production techniques require large-scale system implementations. For future quantum-communication networks, integrable quantum devices would be desirable. However, such devices are not currently available. To reduce the scale of entanglement production, we would like to employ new materials to integrate onto fiber tips or into micro-fabricated quantum devices.

Graphene is a two-dimensional material consisting of a monolayer of carbon atoms arranged in a hexagonal lattice [91]. Much has been learned since people first realized its unusual electronic properties [92, 93]. Graphene has been shown to posses astonishing linear electronic and optical properties, due to its linear and massless band

structure near the Dirac points. For example, electron mobility in graphene reaches 2×10^5 cm^2/Vs, much higher than normal materials such as silicon [94]. Graphene is also the only known material that exhibits an anomalous quantum Hall effect at room temperature [95]. The optical absorption per layer of graphene is related to the fine-structure constant by $\pi\alpha = 2.3\%$ over a broad range of terahertz and optical wavelengths [96–98]. Potential applications include ultra-broadband fast detectors, and the replacement of transparent conductive oxides with epitaxial graphene [46]. Also of interest are potential coherent electronics applications that would use quantum interference of electrons to provide new device functionality.

Besides linear electronic and optical properties, the third-order nonlinear response of materials is useful for certain applications such as wavelength conversion [99] and quantum-entanglement generation [42]. The most important physical parameter for nonlinear-optical experiments is the nonlinear susceptibility of the material. However, in practice, nonlinear-optical experiments are limited by other factors, in particular, the phase-matching conditions arising from wavelength-dependent refractive indices. The accumulation of phase-mismatch as the interacting waves propagate through the nonlinear medium sets a limit on the bandwidth of nonlinear applications. Because the graphene thickness is much less than an optical wavelength, non-critical phase matching occurs, permitting ultra-broadband operation.

The nonlinear properties of graphene have been investigated theoretically in [100–104]. Theoretical results predict that graphene possesses large nonlinearity at the terahertz-frequency [100, 101] and optical-frequency [104] ranges. More recently, the nonlinearity of graphene in the visible-optical range was experimentally measured by four-wave mixing [105]. When taking into account the nonlinear response per unit thickness, the theory adopted in [105] shows that the effective third-order nonlinear susceptibility $\chi^{(3)}$ of graphene is approximately eight orders of magnitude larger than that of glass. The authors in [105] estimated the $\chi^{(3)}$ of graphene by evaluating

the nonlinear surface-current density induced by an external electromagnetic field and by assuming that the dynamic nonlinear response of electrons coupled with an external field is characterized by the electron-photon interaction Hamiltonian. Instead of the dipole-interaction Hamiltonian ($\mathbf{E} \cdot \mathbf{r}$) obtained by the length gauge [105], the minimal-coupling interaction Hamiltonian ($\mathbf{A} \cdot \mathbf{p}$), obtained by the velocity gauge [106], leads to a more convenient way to calculate the carrier-hole-pair generation [107]. Additionally, the quantum dynamics of electrons in graphene are also affected by ultrafast many-body interactions such as electron-electron and electron-phonon scattering [61, 108–110], which in turn may depend on carrier densities, conduction-band energies, and temperature in non-trivial ways, resulting in ultrafast quantum dephasing. Other quantum-dephasing mechanisms may exist. A complete physical model needs to include these effects, which have not yet been included in previous theoretical calculations of the nonlinear susceptibility of graphene.

In this dissertation, a quantum-dynamical model for investigating the quantum dynamics of electrons in graphene will be presented. The electron-photon interaction Hamiltonian is obtained by the minimal substitution in the free-electron Hamiltonian to relate the quantum dynamics of electrons with the vector potential of the electromagnetic field, as in [102]. This work differs in that it includes electron-electron and electron-phonon scattering by introducing two phenomenological decay rates. This work also focuses on nonlinear mixing rather than on the linear decay-free, dephasing-free model. In a quasi-continuous-wave-pump experiment, in which the electron-photon coupling time (order of ps) is much longer than the carrier-relaxation time (order of fs), these phenomenological decay rates allow us to avoid dealing with complicated microscopic quantum-mechanical calculations and to obtain analytical solutions for quantum dynamics of electrons in graphene by exploiting the quantum-perturbation method. The proposed model is appropriate for excitation power well

below the saturation threshold of graphene (4 GW/cm^2) [111], in which case the population inversion for each quantum state in the Brillioun zone does not significantly change. Once the quantum dynamics of electrons in graphene is obtained, both linear and nonlinear optical conductivity produced by different optical processes will be derived.

In this chapter, we first discuss the quantum dynamic of electrons in graphene, which allows us to write the Blochs equations for electrons in graphene. We then present two methods to solve the Blochs equations. The perturbative method enables us to derive analytical solution for the linear and nonlinear optical response of graphene. In the non-perturbative method section, we will address saturation effects in graphene.

5.1 Quantum dynamics of electrons in graphene

In this section, the quantum dynamics of electrons in graphene will be reviewed, starting from first principles. We begin with the free-electron Hamiltonian, obtained for the 2D tight-binding model of a nearest-neighbor-interaction approximation. The electron-photon interaction Hamiltonian is derived later by minimal substitution. We then discuss ultrafast carrier relaxation, which plays an important role in the quantum dynamics of electrons in graphene. The resulting ultrafast quantum dephasing in graphene is accounted for by addition of phenomenological decay rates into the model.

5.1.1 Free-electron Hamiltonian and electron-photon coupling

In the 2D tight-binding model, or the nearest-neighbor-interaction approximation, the motion of electrons is limited by assuming that they can only hop to their nearest neighbors. The Hamiltonian of electrons in graphene under this assumption is written in the second-quantized language [91]:

$$\hat{H} = -\eta \sum_{\langle i,j\rangle,\sigma} (a^{\dagger}_{\sigma,i} b_{\sigma,j} + H.c.), \tag{5.1.1}$$

where $\eta \approx 2.8eV$ is the hopping energy and the product of the creation and annihilation operators $a^{\dagger}_{\sigma,i} b_{\sigma,j}$ represents a process in which an electron with spin $\sigma \in \{\uparrow, \downarrow\}$ is annihilated on site R_i of sublattice A and a new electron of the identical spin is created on its neighbor site R_j of sublattice B. The Fourier transform of the Hamiltonian in Eq. 5.1.1 allows the derivation of the free-electron Hamiltonian in momentum space, which is

$$\hat{H} = \sum_{\mathbf{k}} (a^{\dagger}_{\mathbf{k}} b^{\dagger}_{\mathbf{k}}) H_0 \binom{a_{\mathbf{k}}}{b_{\mathbf{k}}}, \tag{5.1.2}$$

where the summation is performed over the entire Brillioun zone and

$$H_0 = \begin{pmatrix} 0 & h_{\mathbf{p}} \\ h^*_{\mathbf{p}} & 0 \end{pmatrix} \tag{5.1.3}$$

is the first-quantized free-electron Hamiltonian [102], with

$$h_{\mathbf{p}} = -\eta \left[\exp\left(i \frac{a p_y}{\sqrt{3}\hbar} \right) + 2 \cos\left(\frac{a k_x}{2} \right) \exp\left(-i \frac{a p_y}{2\sqrt{3}\hbar} \right) \right], \tag{5.1.4}$$

where $a = 3.3$ Å is the lattice constant of graphene. The first-quantized free-electron Hamiltonian characterizes the quantum dynamics of a single electron with momentum $\mathbf{p} = \hbar \mathbf{k}$.

Energy eigenstates and corresponding eigen-energies can be found by solving the 2D Dirac equation [112]:

$$H_0 |\varphi\rangle = E |\varphi\rangle. \tag{5.1.5}$$

Given the electron momentum $\mathbf{p}$, one finds two energy eigenstates with opposite eigenvalues $E_{C(V)} = \pm |h_{\mathbf{p}}| = \pm v_F p$, corresponding to the conduction-band and valence-band states respectively:

$$|C_{\mathbf{p}}\rangle = \frac{1}{\sqrt{2}} \binom{1}{h^*_{\mathbf{p}}/|h_{\mathbf{p}}|} \tag{5.1.6}$$

$$|V_{\mathbf{p}}\rangle = \frac{1}{\sqrt{2}} \binom{1}{-h^*_{\mathbf{p}}/|h_{\mathbf{p}}|}. \tag{5.1.7}$$

Having discussed the Hamiltonian for a single free electron in graphene, we next derive the Hamiltonian of an electron coupled to an external electromagnetic field,

which is characterized by its vector potential $\widetilde{\mathbf{A}}(t)$, related to the electric field $\mathbf{E}$ and the magnetic field $\mathbf{B}$ by

$$\begin{aligned} \mathbf{E} &= -\frac{\partial \mathbf{A}}{\partial t} \\ \mathbf{B} &= \nabla \times \mathbf{A}. \end{aligned} \tag{5.1.8}$$

Suppose at time $t = 0$, we turn on a homogeneous a.c. electromagnetic field having a vector potential with two polarization components:

$$\widetilde{\mathbf{A}}(t) = \widetilde{A}_x(t)\hat{\mathbf{x}} + \widetilde{A}_y(t)\hat{\mathbf{y}} = \left(\widetilde{A}_x(t), \widetilde{A}_y(t)\right), \tag{5.1.9}$$

where $\hat{\mathbf{x}}$ and $\hat{\mathbf{y}}$ are two orthogonal unit vectors of the Cartesian coordinate system. Each polarization component $\widetilde{A}_q(t)$, $q \in \{x, y\}$, is the summation of different frequency modes on a polarization:

$$\widetilde{A}_q(t) = \sum_n A_{q,n} e^{-i\omega_{q,n}t} = \sum_n \widetilde{A}_{q,n}(t). \tag{5.1.10}$$

Both positive and negative frequencies are allowed. The complex conjugate relation $A_{q,n} = A^*_{q,-n}$ holds to guarantee that the field is real-valued. By using Eq. 5.1.8, we find the electric field with polarization q to be related to the vector potential by

$$\widetilde{E}_q(t) = -\frac{d\widetilde{A}_q(t)}{dt} = \sum_n i\omega_{q,n} A_{q,n} e^{-i\omega_{q,n}t} = \sum_n E_{q,n} e^{-i\omega_{q,n}t}. \tag{5.1.11}$$

The electric-field amplitude and the vector-potential amplitude have the following relation:

$$E_{q,n} = i\omega_{q,n} A_{q,n}. \tag{5.1.12}$$

The electron-photon interaction Hamiltonian can be obtained by the minimal substitution $\mathbf{p} \to \mathbf{p} + e\widetilde{\mathbf{A}}(t)$ on the free-electron Hamiltonian H_0 [59]. The Taylor expansion of the electron-photon interaction Hamiltonian around $\mathbf{p}$ reads

$$H(t) = \begin{pmatrix} 0 & h_{\mathbf{p}} + \nabla h_{\mathbf{p}} \cdot e\widetilde{\mathbf{A}}(t) \\ h^*_{\mathbf{p}} + \nabla h^*_{\mathbf{p}} \cdot e\widetilde{\mathbf{A}}(t) & 0 \end{pmatrix}. \tag{5.1.13}$$

Let $H(t) = H_0 + V(t)$, so that we have

$$V(t) = \begin{pmatrix} 0 & \nabla h_{\mathbf{p}} \cdot e\widetilde{\mathbf{A}}(t) \\ \nabla h^*_{\mathbf{p}} \cdot e\widetilde{\mathbf{A}}(t) & 0 \end{pmatrix} = e \sum_u \widetilde{A}_u(t) \begin{pmatrix} 0 & \frac{\partial h_{\mathbf{p}}}{\partial p_u} \\ \frac{\partial h^*_{\mathbf{p}}}{\partial p_u} & 0 \end{pmatrix}, \tag{5.1.14}$$

where $u \in \{x, y\}$. In the representation of energy eigenstates $|V_{\mathbf{p}}\rangle$ and $|C_{\mathbf{p}}\rangle$, $V(t)$ is organized into the following matrix form:

$$V(t) = \begin{pmatrix} \langle V_{\mathbf{p}}|V(t)|V_{\mathbf{p}}\rangle & \langle V_{\mathbf{p}}|V(t)|C_{\mathbf{p}}\rangle \\ \langle C_{\mathbf{p}}|V(t)|V_{\mathbf{p}}\rangle & \langle C_{\mathbf{p}}|V(t)|C_{\mathbf{p}}\rangle \end{pmatrix} = \sum_{u,j} e\widetilde{A}_{u,j}(t) \begin{pmatrix} V^u_{VV} & V^u_{VC} \\ V^u_{CV} & V^u_{CC} \end{pmatrix}. \tag{5.1.15}$$

In general, the quantum dynamics of an electron can be obtained by solving the time-dependent Schrödinger equation:

$$i\hbar \frac{d\rho}{dt} = [H(t), \rho], \tag{5.1.16}$$

with ρ the density operator of the electron.

5.1.2 Electron relaxation

Eq. 5.1.16 describes the quantum dynamics of an electron with momentum $\mathbf{p}$ that is subject to an external electromagnetic field characterized by its vector potential $\widetilde{\mathbf{A}}(t)$. A valence-band electron can be excited and become a conduction-band electron by absorbing a photon. The transition happens with a particular probability that depends on the field intensity and photon energy. The excited conduction-band electron could be stimulated into the valence band and emit a photon. This whole process is called the Rabi oscillation. However, in a complete physical picture, electrons in the conduction band undergo ultrafast carrier-relaxation processes caused by the faster electron-electron scattering followed by the slower electron-phonon scattering [61, 108, 109]. These scattering processes destroy the quantum coherence of electrons and result in quantum dephasing. In a strong excitation regime, a strong pump pulse depletes the population in the valence band and excites electrons into

the conduction band. Thereafter, the hot electrons in the conduction band undergo an ultrafast electron-electron scattering process (so do the holes in the valence band) that results in quasi-thermalized statistics for electrons in the conduction band, and holes in the valence band. The quasi-thermalized distributions establish new state-occupation probabilities within the two bands. As a result, a strong pump not only changes the state-occupation probability of the state having the corresponding energy, but also affects the state-occupation probabilities over the whole band. A complete treatment that would include the electron-photon, electron-electron, and electron-phonon interactions requires sophisticated quantum-mechanical calculations [61,113]. There may be additional quantum-dephasing processes. However, if we limit ourselves to the steady-state quasi-continuous-wave regime, in which the state-occupation probabilities over the whole bands do not vary with time, the situation is much simpler. To model the ultrafast quantum dephasing in a steady-state quasi-continuous-wave regime, two phenomenological decay rates Γ_1 and Γ_2 are introduced, describing the population and quantum-coherence damping that phenomenologically represent the overall effect of the ultrafast scattering processes. With the two phenomenological decay rates, one arrives at the steady-state Bloch equations for graphene:

$$\begin{aligned}
\dot{\varrho} &= -\Gamma_1(\varrho - \varrho^{eq}) + \frac{2ei}{\hbar}\sum_{u,j}\widetilde{A}_{u,j}(t)[V^u_{VC}(\rho_{VC}+\rho_{CV})] \\
\dot{\rho}_{VC} &= (-i\omega_{VC}-\Gamma_2)\,\rho_{VC} - \frac{ei}{\hbar}\sum_{u,j}\widetilde{A}_{u,j}(t)[2V^u_{VV}\rho_{VC}+V^u_{VC}\rho] \\
\dot{\rho}_{CV} &= (-i\omega_{CV}-\Gamma_2)\,\rho_{CV} - \frac{ei}{\hbar}\sum_{u,j}\widetilde{A}_{u,j}(t)[-2V^u_{VV}\rho_{CV}+V^u_{VC}\rho],
\end{aligned} \tag{5.1.17}$$

where $\varrho = \rho_{CC} - \rho_{VV}$ is the population inversion, $\omega_{CV} = -\omega_{VC} = 2E_C/\hbar$, and ϱ^{eq} is the population inversion in thermal equilibrium. Compared to the Bloch equations for atom vapors and normal semiconductors [60, 61], both diagonal and off-diagonal

driving terms exist for the off-diagonal elements of the density matrix.

5.1.3 Surface-current density in graphene

Macroscopically, the motion of electrons in graphene is characterized by surface current. The optical absorption of graphene is also related to the optical conductivity [97]. Therefore, deriving the optical conductivity plays an important role in understanding the optical response of graphene. Once the density matrix of electrons is obtained by solving Eq. 5.1.17, The expected velocity of the q polarization of a field-coupled electron is given by

$$\langle v^q \rangle = \mathrm{Tr}\left[v^q \rho\right], \tag{5.1.18}$$

where the velocity operator v^q is defined as

$$v^q = \frac{\partial H}{\partial p_q} = \begin{pmatrix} 0 & \frac{\partial h_{\mathbf{p}}}{\partial p_q} \\ \frac{\partial h^*_{\mathbf{p}}}{\partial p_q} & 0 \end{pmatrix} + e\sum_u \widetilde{A}_u(t) \begin{pmatrix} 0 & \frac{\partial^2 h_{\mathbf{p}}}{\partial p_u \partial p_q} \\ \frac{\partial^2 h^*_{\mathbf{p}}}{\partial p_u \partial p_q} & 0 \end{pmatrix} = v'^q + v''^q. \tag{5.1.19}$$

To simplify our discussion, we only consider an external field polarized in the $\hat{x}$ direction with vector potential $\widetilde{A}(t)$.

The velocity operator can then be expressed as

$$v^x = \frac{\partial H}{\partial p_x} = \begin{pmatrix} 0 & \frac{\partial h_{\mathbf{p}}}{\partial p_x} \\ \frac{\partial h^*_{\mathbf{p}}}{\partial p_x} & 0 \end{pmatrix} + e\widetilde{A}(t) \begin{pmatrix} 0 & \frac{\partial^2 h_{\mathbf{p}}}{\partial p_x^2} \\ \frac{\partial^2 h^*_{\mathbf{p}}}{\partial p_x^2} & 0 \end{pmatrix}. \tag{5.1.20}$$

The velocity operator v^x can be transformed into matrix form by evaluating each element in the representation of energy eigenstates, giving

$$v^x = \begin{pmatrix} V^x_{VV} & V^x_{VC} \\ V^x_{CV} & V^x_{CC} \end{pmatrix} + e\widetilde{A}(t) \begin{pmatrix} u^x_{VV} & u^x_{VC} \\ u^x_{CV} & u^x_{CC} \end{pmatrix}, \tag{5.1.21}$$

where

$$\begin{pmatrix} u^x_{VV} & u^x_{VC} \\ u^x_{CV} & u^x_{CC} \end{pmatrix} = \frac{1}{2|h_{\mathbf{p}}|} \begin{pmatrix} -h^*_{\mathbf{p}} \frac{\partial^2 h_{\mathbf{p}}}{\partial p_x^2} - h_{\mathbf{p}} \frac{\partial^2 h^*_{\mathbf{p}}}{p_x^2} & h^*_{\mathbf{p}} \frac{\partial^2 h_{\mathbf{p}}}{\partial p_x^2} - h_{\mathbf{p}} \frac{\partial^2 h^*_{\mathbf{p}}}{p_x^2} \\ h_{\mathbf{p}} \frac{\partial^2 h^*_{\mathbf{p}}}{\partial p_x^2} - h^*_{\mathbf{p}} \frac{\partial^2 h_{\mathbf{p}}}{p_x^2} & h^*_{\mathbf{p}} \frac{\partial^2 h_{\mathbf{p}}}{\partial p_x^2} + h_{\mathbf{p}} \frac{\partial^2 h^*_{\mathbf{p}}}{p_x^2} \end{pmatrix}. \tag{5.1.22}$$

A similar derivation can be found in [107, 112].

The surface current in the q direction is obtained by an integral over the whole Brillioun zone:

$$\widetilde{J}^q(t) = \frac{1}{4\pi^2}\int_{\mathbf{BZ}} -e\langle v^q\rangle dk_x dk_y. \tag{5.1.23}$$

In general, $\widetilde{J}^q(t)$ contains a linear contribution whose oscillating frequency equals the optical frequency, and also a nonlinear contribution whose oscillating frequency is the combination of the incoming optical-frequency components. In the next sections, the optical response of graphene will be derived analytically by a perturbative method and numerically by a non-perturbative method. Once graphene is subject to an external electromagnetic field, the quantum dynamics of electrons is determined by Eq. 5.1.17 in general. However, Eq. 5.1.17 can not be solved analytically in general. To obtain a solution, we require either additional assumptions to acquire an analytical solution or numerical calculations for more general situations. The perturbative method will first be discussed. For the perturbative method, analytical solutions are derived under the ideal Dirac fermion assumption. The solutions are only valid under low excitation power. The non-perturbative method, which requires numerical calculations, is more generally valid and can be used to predict saturation effects in graphene, as well as the linear and nonlinear response.

5.2 Perturbative method

Under the ideal Dirac fermion assumption, in the vicinities of two Dirac points $\mathbf{K}^{\pm}$ in the Brillioun zone, we have the following linear dispersion relation for $h_{\mathbf{p}}$:

$$h_{\mathbf{p}} = v_F(p_x \mp ip_y) = v_F p(\cos\theta \mp i\sin\theta), \tag{5.2.1}$$

where $v_F \approx 10^6$ m/s is the Fermi velocity of electrons in graphene. The matrix components in Eq. 5.1.15 are also reformulated to be

$$\begin{aligned} V^x_{VV} &= -v_F \cos\theta, V^x_{VC} = \pm i v_F \sin\theta, V^x_{CV} = \mp i v_F \sin\theta, V^x_{CC} = v_F \cos\theta \\ V^y_{VV} &= -v_F \sin\theta, V^y_{VC} = \mp i v_F \cos\theta, V^y_{CV} = \pm i v_F \cos\theta, V^y_{CC} = v_F \sin\theta. \end{aligned} \tag{5.2.2}$$

The perturbative method gives the solution in the following cascaded form in the frequency domain, with each order denoted by a positive index k:

$$\begin{aligned} \dot{\varrho}^{(k+1)} &= -\Gamma_1 \varrho^{(k+1)} + \frac{2ei}{\hbar} \sum_{u,j} \widetilde{A}_{u,j}(t)[V^u_{VC}(\rho^{(k)}_{VC} + \rho^{(k)}_{CV})] \\ \dot{\rho}^{(k+1)}_{VC} &= (-i\omega_{VC} - \Gamma_2)\, \rho^{(k+1)}_{VC} - \frac{ei}{\hbar} \sum_{u,j} \widetilde{A}_{u,j}(t)[2V^u_{VV}\rho^{(k)}_{VC} + V^u_{VC}\rho^{(k)}] \\ \dot{\rho}^{(k+1)}_{CV} &= (-i\omega_{CV} - \Gamma_2)\, \rho^{(k+1)}_{CV} - \frac{ei}{\hbar} \sum_{u,j} \widetilde{A}_{u,j}(t)[-2V^u_{VV}\rho^{(k)}_{CV} + V^u_{VC}\rho^{(k)}], \end{aligned} \tag{5.2.3}$$

for $k > 0$. Finding the solution is simplified by transforming Eq. 5.2.3 into frequency domain by means of the Laplace transform, which results in

$$\begin{aligned} \varrho^{(k+1)}(\Omega) &= \frac{e}{\hbar} \sum_{u,j} \frac{2A_{u,j}}{(\Omega - i\Gamma_1)} V^u_{VC} \left[\rho^{(k)}_{VC}(\Omega + \omega_{u,j}) + \rho^{(k)}_{CV}(\Omega + \omega_{u,j})\right] \\ \rho^{(k+1)}_{VC}(\Omega) &= -\frac{e}{\hbar} \sum_{u,j} \frac{A_{u,j}}{(\Omega + \omega_{VC} - i\Gamma_2)} \left[2V^u_{VV}\rho^{(k)}_{VC}(\Omega + \omega_{u,j}) + V^u_{VC}\varrho^{(k)}(\Omega + \omega_{u,j})\right] \\ \rho^{(k+1)}_{CV}(\Omega) &= -\frac{e}{\hbar} \sum_{u,j} \frac{A_{u,j}}{(\Omega + \omega_{CV} - i\Gamma_2)} \left[-2V^u_{VV}\rho^{(k)}_{CV}(\Omega + \omega_{u,j}) + V^u_{VC}\varrho^{(k)}(\Omega + \omega_{u,j})\right], \end{aligned} \tag{5.2.4}$$

where $\Omega = \omega - i\kappa$ with $\kappa > 0$ in order for the Laplace transform to converge.

5.2.1 Linear optical conductivity

The zeroth-order solution to the density matrix is simply the thermal-equilibrium values of the population inversion and quantum coherence. At temperature $T = 0$, we have $\rho^{(0)}_{CC} = \rho^{(0)}_{VC} = \rho^{(0)}_{CV} = 0$, $\rho^{(0)}_{VV} = 1$. Inserting zeroth-order solution into Eq.

5.2.4 leads to the first-order solution:

$$\begin{aligned}
\varrho^{(1)}(\Omega) &= 0 \\
\rho^{(1)}_{VC}(\Omega) &= \frac{e}{\hbar}\cdot\frac{1}{(\Omega+\omega_{VC}-i\Gamma_2)}\sum_{w,n}V^{w}_{VC}\widetilde{A}_{w,n}(\Omega) \\
\rho^{(1)}_{CV}(\Omega) &= \frac{e}{\hbar}\cdot\frac{1}{(\Omega+\omega_{CV}-i\Gamma_2)}\sum_{w,n}V^{w}_{VC}\widetilde{A}_{w,n}(\Omega),
\end{aligned} \tag{5.2.5}$$

where $\widetilde{A}_{w,n}(\Omega)$ is the Laplace transform of the time-dependent vector potential of one frequency mode indexed by n on polarization w. The linear electron velocity is contributed by both the diagonal elements from $\rho^{(0)}$ and the off-diagonal elements from $\rho^{(1)}$ [107, 112]:

$$\langle v^x\rangle_l = \mathrm{Tr}\left[v'^x\rho^{(1)} + v''^x\rho^{(0)}\right]. \tag{5.2.6}$$

The linear surface-current density $\widetilde{J}_l(\Omega)$ can be obtained by integration over the whole Brillouin zone. Since the integrand $\langle v^x\rangle_l$ is only appreciable in the vicinity of the input optical frequency ω, instead of an integral limited in the Brillioun zone, we can extend the integral to infinity without significantly affecting the result. The integral is written as

$$\begin{aligned}
\widetilde{J}_l(\Omega) &= \frac{1}{4\pi^2}\int_0^{2\pi}d\theta\int_0^{\infty}-e\langle v^x\rangle_l k dk \\
&= -i\frac{e^2}{16\hbar}(\Omega-i\Gamma_2)\widetilde{A}(\Omega).
\end{aligned} \tag{5.2.7}$$

By using the frequency-domain relation $\widetilde{E}(\Omega) = -i\Omega\widetilde{A}(\Omega)$, the linear optical conductivity is derived as

$$\sigma_l = 4\times\frac{e^2}{16\hbar}\left(1+\frac{\Gamma_2}{\omega}i\right) = \sigma_0\left(1+\frac{\Gamma_2}{\omega}i\right), \tag{5.2.8}$$

where σ_0 is the theoretical prediction of the universal optical conductivity of graphene [96–98]. A factor 4 is added due to valley and spin degeneracies. If we compare Eq. 5.2.8 with the experimental measurements of the complex optical conductivity of graphene at $\lambda = 550$nm in [114–116], we find that Γ_2 ranges from 1.39×10^{15} s^{-1} to 4×10^{15} s^{-1} by normalizing the real parts to σ_0.

In [117], the authors ascribe the imaginary part of the conductivity of graphene to the virtual transition of electrons at M and Γ points in the Brillioun zone. However, our quantum mechanical calculations based on the nearest-neighbor-interaction approximation find that we have $\nabla h_{\mathbf{p}} = 0$ at the Γ point, leading to a zero interaction Hamiltonian, i.e., $V(t) = 0$. At the M point, the interaction Hamiltonian gives pure real diagonal elements, and pure imaginary off-diagonal elements as in Eq. 5.1.15. Thus, the conductivity at the M point is still real as long as we set $\Gamma_1 = \Gamma_2 = 0$. Thus it seems that the relatively large imaginary part of the conductivity arises from the ultrafast quantum dephasing in graphene. The fact that this time constant is approximately 1 fs indicates both that optical measurements can be used to characterize quantum dephasing in particular samples and that dipole quantum coherence would seem to be a poor candidate for coherent electron devices in graphene.

5.2.2 Nonlinear optical conductivity

To evaluate the nonlinear interactions in graphene, we need to solve for higher-order density-matrix terms $\rho^{(2)}$ and $\rho^{(3)}$. Having obtained $\rho^{(2)}$ and $\rho^{(3)}$, the expected nonlinear velocity on polarization q for an electron with momentum $\mathbf{p}$ can be calculated as

$$\langle v^q \rangle_{nl} = \mathrm{Tr}\left[v^q \rho^{(3)}\right]. \tag{5.2.9}$$

According to Eq. 5.1.19, both $\rho^{(2)}$ and $\rho^{(3)}$ contribute to $\langle v^q \rangle_{nl}$. To derive the nonlinear surface-current density, we need to integrate over the entire Brillouin zone. $\rho^{(2)}$ and $\rho^{(3)}$ both are appreciable only in the vicinities of their resonant frequencies. The contribution from $\rho^{(2)}$ can be neglected since the second derivative of $h_{\mathbf{p}}$ gives zero due to the linear band structure of graphene near the Dirac points. Thus, in the nonlinear surface-current-density calculation, we only keep the v'^q term and drop the v''^q term in Eq. 5.1.19. The resulting nonlinear velocity is written as

$$\langle v^q \rangle_{nl} = \mathrm{Tr}\left[v'^q \rho^{(3)}\right] = \sum_{u,l}\sum_{v,m}\sum_{w,n}\langle v^q_{u,l;v,m;w,n}\rangle, \tag{5.2.10}$$

where the expected velocity of one frequency component of polarization q is defined as $\langle v^q_{u,l;v,m;w,n}\rangle$. Since the main contribution of $\langle v^q_{u,l;v,m;w,n}\rangle$ comes from the vicinities of each resonant frequency, we can extend the integration in the Brillouin zone to infinity and without significantly affecting the result. By assuming the Dirac cone goes to infinity, we obtain analytical solutions to the third-order surface-current density of one frequency component having polarization q to be

$$\begin{aligned}\widetilde{J}^q_{u,l;v,m;w,n}(\Omega) &= \frac{1}{4\pi^2}\int_0^{2\pi} d\theta \int_0^{\infty} -e\langle v^q_{u,l;v,m;w,n}\rangle k dk \\ &= -i\frac{v_F^2 e^4}{16\hbar^3} A_{u,l}A_{v,m}\left[\frac{\mu_{q,u,v,w}}{\Omega - i\Gamma_1} + \right. \\ &\quad \left.\frac{\nu_{q,u,v,w}(\Omega+\omega_{u,l}+\omega_{v,m}-i\Gamma_2)}{(\Omega+\omega_{u,l}-i\Gamma_1)(2\Omega+\omega_{u,l}+\omega_{v,m}-2i\Gamma_2)}\right]\times \\ &\quad \widetilde{A}_{w,n}(\Omega+\omega_{u,l}+\omega_{v,m}),\end{aligned} \tag{5.2.11}$$

where $\mu_{q,u,v,w}$ and $\nu_{q,u,v,w}$ are

$$\begin{aligned}\mu_{q,u,v,w} &= \frac{4}{\pi v_F^4}\int_0^{2\pi} V^q_{VV}V^u_{VC}V^v_{VV}V^w_{VC}d\theta \\ \nu_{q,u,v,w} &= \frac{4}{\pi v_F^4}\int_0^{2\pi} V^q_{VC}V^u_{VC}V^v_{VC}V^w_{VC}d\theta.\end{aligned} \tag{5.2.12}$$

In the time domain, the steady-state solution to the nonlinear surface-current density is

$$\begin{aligned}\widetilde{J}^q_{u,l;v,m;w,n}(t) &= 4\times\frac{v_F^2e^4}{16\hbar^3}\frac{E_{u,l}E_{v,m}E_{w,n}}{\omega_{u,l}\omega_{v,m}\omega_{w,n}}\left[\frac{\mu_{q,u,v,w}}{(\omega_{u,l}+\omega_{v,m}+\omega_{w,n}+i\Gamma_1)}\right. \\ &+ \left.\frac{\nu_{q,u,v,w}(\omega_{w,n}+i\Gamma_2)}{(\omega_{u,l}+\omega_{v,m}+2\omega_{w,n}+2i\Gamma_2)(\omega_{v,m}+\omega_{w,n}+i\Gamma_1)}\right]e^{-i(\omega_{u,l}+\omega_{v,m}+\omega_{w,n})t},\end{aligned} \tag{5.2.13}$$

where a coefficient of 4 is added to include valley and spin degeneracies. We have substituted the vector-potential amplitude with the electric-field amplitude by use of Eq. 5.1.12. Having obtained the surface-current density of one frequency component

$\widetilde{J}^q_{u,l;v,m;w,n}(t)$ of polarization q, the total surface-current density for this polarization is the summation over all frequency components,

$$\widetilde{J}^q_{nl}(t) = \sum_{u,l}\sum_{v,m}\sum_{w,n}\widetilde{J}^q_{u,l;v,m;w,n}(t). \tag{5.2.14}$$

Eq. 5.2.14 is a general expression for the total third-order nonlinear surface-current density, composed of different frequency modes, each of which is produced by a particular nonlinear-optical process. For example, let $\omega_{p_1}, \omega_{p_2}$ be the frequencies of the pump modes and ω_s be the frequency of the signal mode, the frequency $3\omega_{p_1}$ results from third-harmonic generation of the pump at frequency ω_{p_1} while $\omega_i = \omega_{p_1} + \omega_{p_2} - \omega_s$ is produced by four-wave mixing.

We mark one frequency mode with frequency ω on polarization q as $\widetilde{J}^q_\omega(t)$. $\widetilde{J}^q_\omega(t)$ is the summation over all frequency components $\widetilde{J}^q_{u,l;v,m;w,n}(t)$ satisfying $\omega_{u,l} + \omega_{v,m} + \omega_{w,n} = \omega$:

$$\widetilde{J}^q_\omega(t) = \sum_{\omega_{u,l}+\omega_{v,m}+\omega_{w,n}=\omega}\widetilde{J}^q_{u,l;v,m;w,n}(t) = J^q_\omega e^{-i\omega t}. \tag{5.2.15}$$

5.2.3 Four-wave mixing in graphene

Of particular interest is the study of four-wave mixing, a nonlinear-optical process involving four modes. Two of these serve as the pump modes- one as the signal mode, and one as the idler mode. The optical frequencies ω_{p_1} and ω_{p_2} correspond to the two pump modes, ω_s to the signal mode, and ω_i to the idler mode. Energy conservation gives $\omega_{p_1} + \omega_{p_2} = \omega_s + \omega_i$. Microscopically, four-wave mixing is a process in which two pump photons are annihilated while one signal and one idler photon are created. In the special case where the two pump modes share the same optical frequency, i.e., $\omega_{p_1} = \omega_{p_2} = \omega_p$, the four-wave mixing is pump degenerate. Since four-wave mixing is a third-order nonlinear process, its strength in the electric field is proportional to the nonlinear susceptibility $\chi^{(3)}$. If the frequency of the optical modes are far away from the resonant frequency of the nonlinear medium, the results is a non-resonant

susceptibility $\chi^{(3)}_{\rm NR}$. In the quantum-mechanical picture, $\chi^{(3)}_{\rm NR}$ arises from the fact that the photon energies are far from the bandgap of the nonlinear medium. A typical value for the non-resonant susceptibility in optical fibers is $\chi^{(3)}_{\rm NR} \sim 10^{-15}$ esu [60]. However, a much higher $\chi^{(3)}$ [118,119] is present if the bandgap of the nonlinear medium is close to the interacting-photon energies. The resonance-enhanced nonlinear susceptibility $\chi^{(3)}_{\rm R}$ is typically of the order of 10^{-7} esu.

Graphene is a zero-bandgap semiconductor with a linear band structure near the Dirac points, making it "more resonant" than typical resonant media. The zero bandgap of graphene results in the fact that any frequency within the range from DC to optical frequencies is resonant, which is the physical origin of the high and uniform absorption of graphene. While absorption is a resonance-enhanced linear process, nonlinear processes can also be enhanced by resonance. In particular, four-wave mixing in graphene can be enhanced by the five resonance-enhanced processes plotted in Figure 46. Different resonance-enhanced four-wave mixing processes exist simultaneously for electrons with different energies in graphene. We next discuss these resonance-enhanced four-wave mixing processes.

(a) Two-photon absorption enhanced four-wave mixing: Two-photon absorption happens when the bandgap of a material is twice the photon energy of the incident light. In graphene, this corresponds to $\omega_{CV} \simeq 2\omega_p$.

(b) One-photon pump absorption enhanced four-wave mixing: Unlike two-photon absorption, in which one electron is excited by two incoming photons simultaneously, an electron is excited by a single photon in a one-photon absorption process. In graphene, the condition for one-photon absorption is $\omega_{CV} \simeq \omega_p$.

(c) Idler-enhanced four-wave mixing: In four-wave mixing, if the emitted light frequency, i.e., ω_i, is close the the bandgap of the nonlinear medium, a resonance-enhanced effect also exists. In graphene, this happens at the bandgap $\omega_{CV} = \omega_i$.

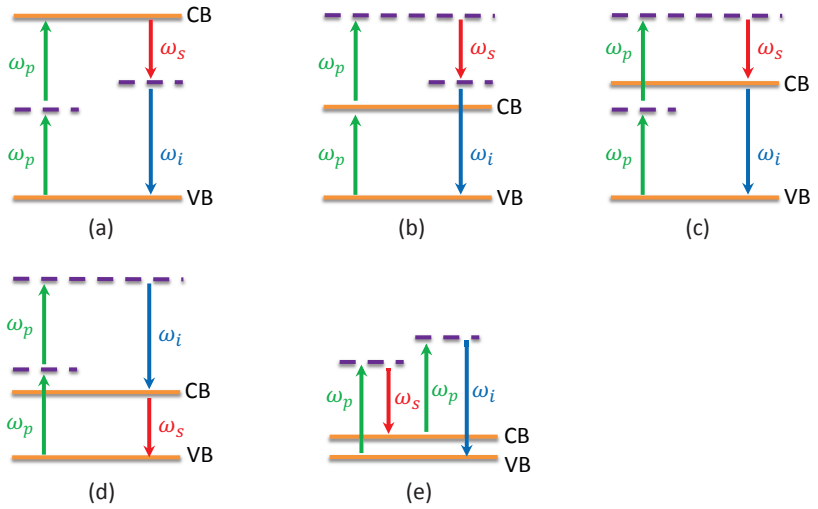


Figure 46: Five resonance-enhanced four-wave mixing processes in graphene. (a) Two-photon absorption enhanced four-wave mixing. (b) One-photon absorption enhanced four-wave mixing. (c) Idler resonance-enhanced four-wave mixing. (d) Signal resonance-enhanced four-wave mixing. (e) Detuning-enhanced four-wave mixing.

(d) Signal-enhanced four-wave mixing: If the signal-photon energy is close to the bandgap of the nonlinear medium, we also have an enhanced effect for four-wave mixing. In graphene, signal-enhanced four-wave mixing happens at bandgap $\omega_{CV} = \omega_s$.

(e) Detuning-enhanced four-wave mixing: Detuning-enhanced four-wave mixing in graphene is similar to the four-wave mixing enhancement by coherent anti-Stokes Raman scattering [120, 121], when the frequency detuning between the pump mode and the Stokes mode is close to the molecule-vibration energy. In graphene, this is the case when the bandgap is close to the frequency detuning between the pump and the signal, i.e., $\omega_{CV} \simeq \omega_p - \omega_s$.

5.2.3.1 *Non-degenerate four-wave mixing*

(A) *Co-polarized* non-degenerate four-wave mixing

In the co-polarized case, we let all frequency modes be $\hat{x}$ polarized. We define the conductivity of the co-polarized non-degenerate four-wave mixing as

$$\widetilde{J}^x_{\mathrm{CN}}(t) = \sigma_{\mathrm{CN}} E_{p_1} E_{p_2} E_s^* e^{-i\omega_i t} + \text{c.c.} = \widetilde{J}^x_{\omega_i}(t) + \widetilde{J}^x_{-\omega_i}(t). \tag{5.2.16}$$

The frequency components contributing to σ_{CN} are listed in Table 4. We insert terms

Table 4: Frequency components for co-polarized non-degenerate four-wave mixing

$\omega_{u,l}$	$\omega_{v,m}$	$\omega_{w,n}$	$\mu_{x,u,v,w}$	$\nu_{x,u,v,w}$
x, ω_{p_1}	x, ω_{p_2}	$x, -\omega_s$	-1	3
x, ω_{p_2}	x, ω_{p_1}	$x, -\omega_s$	-1	3
x, ω_{p_1}	$x, -\omega_s$	x, ω_{p_2}	-1	3
x, ω_{p_2}	$x, -\omega_s$	x, ω_{p_1}	-1	3
$x, -\omega_s$	x, ω_{p_1}	x, ω_{p_2}	-1	3
$x, -\omega_s$	x, ω_{p_2}	x, ω_{p_1}	-1	3

in Table 4 into Eq. 5.2.13 and Eq. 5.2.15 to obtain

$$\sigma_{\mathrm{CN}} = \frac{8}{3} \times \frac{J^x_{\omega_i}}{E_{p_1} E_{p_2} E_s^*}, \tag{5.2.17}$$

where the coefficient $\frac{8}{3}$ comes from standard definition of third-order susceptibility [122].

(B) *Cross-polarized* non-degenerate four-wave mixing

For cross-polarized non-degenerate four-wave mixing, two pump modes at frequencies ω_{p_x} and ω_{p_y} are on orthogonal polarizations $\hat{x}$ and $\hat{y}$. We assume that the signal mode at frequency ω_s is polarized on $\hat{x}$. Momentum conservation guarantees that the idler mode is produced on the $\hat{y}$ polarization. We define the conductivity for this nonlinear process to be

$$J^y_{\mathrm{XN}}(t) = \sigma_{\mathrm{XN}} E_{p_x} E_{p_y} E_s^* e^{-i\omega_i t} + \text{c.c.} = J^y_{\omega_i}(t) + J^y_{-\omega_i}(t). \tag{5.2.18}$$

Table 5: Frequency components for cross-polarized non-degenerate four-wave mixing

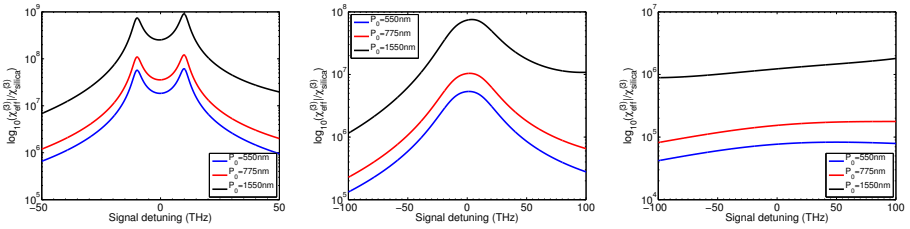
$\omega_{u,l}$	$\omega_{v,m}$	$\omega_{w,n}$	$\mu_{y,u,v,w}$	$\nu_{y,u,v,w}$
x, ω_{p_x}	y, ω_{p_y}	$x, -\omega_s$	-3	1
y, ω_{p_y}	x, ω_{p_x}	$x, -\omega_s$	1	1
x, ω_{p_x}	$x, -\omega_s$	y, ω_{p_y}	1	1
$x, -\omega_s$	x, ω_{p_x}	y, ω_{p_y}	1	1
y, ω_{p_y}	$x, -\omega_s$	x, ω_{p_x}	1	1
$x, -\omega_s$	y, ω_{p_y}	x, ω_{p_x}	-3	1

The contributing frequency components to σ_{XN} are listed in Table 5. By comparing Table 5 with Table 4, we find that $\sigma_{\mathrm{XN}} = \frac{1}{3}\sigma_{\mathrm{CN}}$. Thus, σ_{XN} and σ_{CN} differ only by a factor of 3 as in typical nonlinear media. We can adopt the same approach as in [105] to compare the effective third-order susceptibility of graphene with the third-order susceptibility of silica. The effective third-order susceptibility of graphene is given in the MKS units by

$$\chi^{(3)}_{\mathrm{eff}} = \frac{|\sigma_{\mathrm{CN}}|}{\epsilon_0 \omega_i d}, \tag{5.2.19}$$

where $d \simeq 3.3$Å is the effective thickness of a monolayer of graphene. A typical value for the non-degenerate non-resonant third-order susceptibility of silica such as glass is $\chi^{(3)}_{\mathrm{silica}} = 0.64 \times 10^{-22}$ m^2/V^2 around 550 nm, $\chi^{(3)}_{\mathrm{silica}} = 0.92 \times 10^{-22}$ m^2/V^2 around 775 nm, and $\chi^{(3)}_{\mathrm{silica}} = 1.04 \times 10^{-22}$ m^2/V^2 around 1550 nm. [123]. We plot the ratio between the two susceptibilities in Figures 47 in semi-log scales. In each figure, the three curves correspond to center pump wavelengths at 550 nm, 775 nm, and 1550 nm respectively. For each center pump wavelength, we choose three detuning frequencies of 10 THz, 20 THz, and 30 THz between the two pump modes.

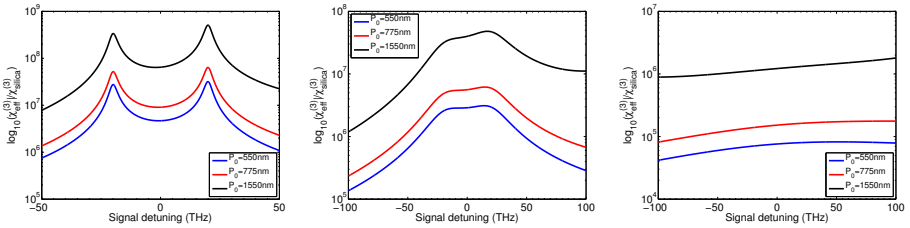
Although [105] predicts that the nonlinear susceptibility of graphene is approximately 8 orders of magnitude greater than that of insulators, our more complete model shows that the ratio between the two susceptibilities can vary from 5 to 9 orders of magnitude, depending on the pump wavelengths, the signal detuning, and the



(a) Pump detuning from the center 10THz. $\Gamma_1 = \Gamma_2 = 10^{13}$.

(b) Pump detuning from the center 10THz. $\Gamma_1 = \Gamma_2 = 10^{14}$.

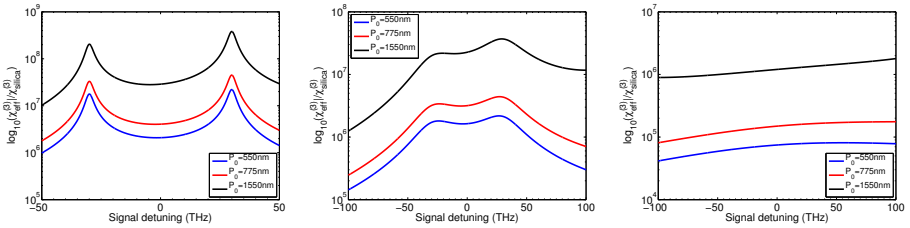
(c) Pump detuning from the center 10THz. $\Gamma_1 = \Gamma_2 = 10^{15}$.



(d) Pump detuning from the center 20THz. $\Gamma_1 = \Gamma_2 = 10^{13}$.

(e) Pump detuning from the center 20THz. $\Gamma_1 = \Gamma_2 = 10^{14}$.

(f) Pump detuning from the center 20THz. $\Gamma_1 = \Gamma_2 = 10^{15}$.



(g) Pump detuning from the center 30THz. $\Gamma_1 = \Gamma_2 = 10^{13}$.

(h) Pump detuning from the center 30THz. $\Gamma_1 = \Gamma_2 = 10^{14}$.

(i) Pump detuning from the center 30THz. $\Gamma_1 = \Gamma_2 = 10^{15}$.

Figure 47: The ratio between the third-order susceptibility of graphene and that of glass. $\chi^{(3)}_{\mathbf{eff}}$ is calculated from the nonlinear optical conductivity of non-degenerate co-polarized four-wave mixing for different pump detunings and decay rates Γ_1 and Γ_2. P_0 denotes the center wavelength between the two pumps.

decay rates Γ_1 and Γ_2. A faster quantum dephasing results in a lower nonlinearity due to the fact that the coherence of electrons is quickly destroyed by the environment via scattering processes. Our theory also predicts that as the pump-signal detuning becomes smaller, the strength of four-wave mixing increases due to the resonance-enhanced effect. Another interesting phenomenon is that as the quantum dephasing times approach $\sim$ 1 fs, the typical symmetry in the nonlinear susceptibility breaks

down.

5.2.3.2 Degenerate four-wave mixing

The optical conductivity for degenerate four-wave mixing can be obtained by setting $\omega_{p_1} = \omega_{p_2} = \omega_p$ in the derivation of the non-degenerate four-wave mixing conductivity and dividing the result by 2 to account for degeneracy. In experiments, the observed idler photon-current intensity I relates to the degenerate four-wave mixing conductivity σ_{D} by

$$I \propto |E_p^2 E_s^* \sigma_{\mathrm{D}}|^2, \tag{5.2.20}$$

with σ_{D} as a function of ω_p, ω_s, Γ_1, and Γ_2. In Figure 48 we compare the idler photon-current intensity predicted by Eq. 5.2.20 with that predicted by Eq. 4 in [105]. Depending on the decay rates Γ_1 and Γ_2, the ratio between the two current intensities varies. The result shows that faster quantum-dephasing rates lead to a weaker four-wave mixing. For decay rates at 10^{15} s^{-1}, the four-wave-mixing photon-current intensity is 200 times higher than what was predicted by Eq. 4 in [105].

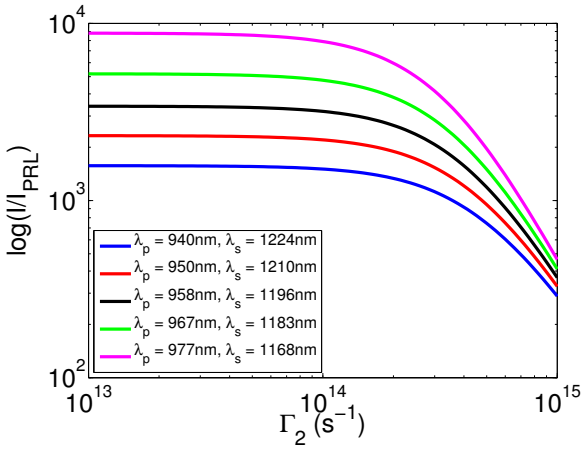


Figure 48: The four-wave-mixing current intensity ratio between Eq. 5.2.20 and the theoretical result in [105]. Five curves corresponds to five different pump and signal wavelengths in [105]. We set $\Gamma_1 = \Gamma_2/2$. Both the ratio and the decay constants are plotted in logarithm scale.

5.3 Non-perturbative method

The perturbative method used in Sec. 5.2 gives a good approximation under low-excitation power, or equivalently, when the population inversion ϱ is close to ϱ^{eq}. With high excitation power, however, the population inversion ϱ diverges significantly from ϱ^{eq} and the perturbative method fails, and we start to see saturation. Classically, a saturable physical quantity Q is related to the input intensity I and the saturation threshold I_{th} by [60]

$$Q = \frac{Q_0}{1 + I/I_{\text{th}}}, \tag{5.3.1}$$

where Q_0 is the non-saturating value. In graphene, we expect a similar saturating behavior. For the two-level model in classical nonlinear optics [60], once the detuning and decay rates are small compared to the optical frequencies, the rotating-wave approximation can be exploited, allowing us to get analytical solutions for the saturation effect. More generally, Eq. 5.1.17 can be numerically solved with any detuning and decay rates. To make the discussion simpler, we limit ourselves to the case where the pump and the signal are co-polarized in the x direction and we seek steady-state solutions only. Under these restrictions, Eq. 5.1.17 becomes

$$\begin{aligned}
\dot{\varrho} &= -\Gamma_1 (\varrho - \varrho^{eq}) \\
&+ \frac{2ie}{\hbar} \sum_j \widetilde{A}_j(t) V_{VC} (\rho_{VC} + \rho_{CV}) \\
\dot{\rho}_{VC} &= (i\omega_{CV} - \Gamma_2) \rho_{VC} \\
&- \frac{ie}{\hbar} \sum_j \widetilde{A}_j(t) [2V_{VV}\rho_{VC} + V_{VC}\varrho] \\
\dot{\rho}_{CV} &= (-i\omega_{CV} - \Gamma_2) \rho_{CV} \\
&- \frac{ie}{\hbar} \sum_j \widetilde{A}_j(t) [-2V_{VV}\rho_{CV} + V_{VC}\varrho] ,
\end{aligned} \tag{5.3.2}$$

where $j \in \{p, s\}$ denoting the pump or the signal mode. The values for V_{VC} and V_{VV} can be obtained numerically from Eq. 5.1.15. ϱ, ρ_{VC}, and ρ_{CV} are composed of

several frequency components with frequencies $m\omega_p + n\omega_s$. We let

$$\begin{aligned}
\varrho(t) &= \sum_{m,n} \varrho^{(m,n)}(t) e^{-i(m\omega_p + n\omega_s)t} + \text{c.c.} \\
\rho_{VC}(t) &= \sum_{m,n} \rho_{VC}^{(m,n)}(t) e^{-i(m\omega_p + n\omega_s)t} + \text{c.c.} \\
\rho_{CV}(t) &= \sum_{m,n} \rho_{CV}^{(m,n)}(t) e^{-i(m\omega_p + n\omega_s)t} + \text{c.c.}
\end{aligned} \tag{5.3.3}$$

The steady-state condition yields

$$\dot{\varrho}(t) = \dot{\rho_{VC}}(t) = \dot{\rho_{CV}}(t) = 0. \tag{5.3.4}$$

By substituting Eq. 5.3.3 and using Eq. 5.3.4, the amplitudes for different frequency components are related by

$$\begin{aligned}
&\left[-\Gamma_1 + i\left(m\omega_p + n\omega_s\right)\right] \rho^{(m,n)} + \frac{2ieV_{VC}}{\hbar} \\
&\left(A_p \rho_{VC}^{(m-1,n)} + A_p^* \rho_{VC}^{(m+1,n)} + A_s \rho_{VC}^{(m,n-1)} + A_s^* \rho_{VC}^{(m,n+1)}\right. \\
&\left. + A_p \rho_{CV}^{(m-1,n)} + A_p^* \rho_{CV}^{(m+1,n)} + A_s \rho_{CV}^{(m,n-1)} + A_s^* \rho_{CV}^{(m,n+1)}\right) = -\Gamma_1 \varrho^{eq} \delta_{m,0} \delta_{n,0}
\end{aligned} \tag{5.3.5a}$$

$$\begin{aligned}
&\left[-\Gamma_2 + i\left(m\omega_p + n\omega_s + \omega_{CV}\right)\right] \rho_{VC}^{(m,n)} \\
&- \frac{ie}{\hbar}\left[2V_{VV}\left(A_p \rho_{VC}^{(m-1,n)} + A_p^* \rho_{VC}^{(m+1,n)} + A_s \rho_{VC}^{(m,n-1)} + A_s^* \rho_{VC}^{(m,n+1)}\right)\right. \\
&\left. + V_{VC}\left(A_p \varrho^{(m-1,n)} + A_p^* \varrho^{(m+1,n)} + A_s \varrho^{(m,n-1)} + A_s^* \varrho^{(m,n+1)}\right)\right] = 0
\end{aligned} \tag{5.3.5b}$$

$$\begin{aligned}
&\left[-\Gamma_2 + i\left(m\omega_p + n\omega_s - \omega_{CV}\right)\right] \rho_{CV}^{(m,n)} \\
&- \frac{ie}{\hbar}\left[-2V_{VV}\left(A_p \rho_{CV}^{(m-1,n)} + A_p^* \rho_{CV}^{(m+1,n)} + A_s \rho_{CV}^{(m,n-1)} + A_s^* \rho_{CV}^{(m,n+1)}\right)\right. \\
&\left. + V_{VC}\left(A_p \varrho^{(m-1,n)} + A_p^* \varrho^{(m+1,n)} + A_s \varrho^{(m,n-1)} + A_s^* \varrho^{(m,n+1)}\right)\right] = 0.
\end{aligned} \tag{5.3.5c}$$

Eq. 5.3.5 consists of an infinite number of frequency modes. To obtain numerical solutions, higher-order modes need to be truncated since their amplitudes are negligible.

We let $|m| \leq m_{max}, |n| \leq n_{max}$. The truncation ends up with $3(2m_{max}+1)(2n_{max}+1)$ unknowns, which are later solved by linear algebra. The surface-current density is then obtained by

$$\begin{aligned} \widetilde{J}(t) &= \frac{1}{4\pi^2}\int_{\mathbf{BZ}} -e\langle v^x\rangle dk_x dk_y. \\ &= \sum_{m,n} J^{(m,n)} e^{-i(m\omega_p+n\omega_s)t} + \text{c.c.}, \end{aligned} \tag{5.3.6}$$

where v^x can be reorganized into matrix form as Eq. 5.1.21 and is evaluated by numerical calculation of the two matrices in the equation.

5.3.1 Linear optical conductivity

For the linear optical conductivity, we define

$$\sigma_l = 2 \times \frac{J^{(1,0)}}{E_p} \tag{5.3.7}$$

as the linear conductivity, which is composed of both a real part and an imaginary part. The coefficient 2 is to include the spin degeneracy. The real part contributes to absorption and the imaginary part results in a phase shift. In Figure 49, we fit our theory to the experimental transmittance data obtained in [96], which gives $\tau_2 = 1/\Gamma_2 = \approx 0.64$ fs. The wavelength dependence of the real part is plotted in Fig-

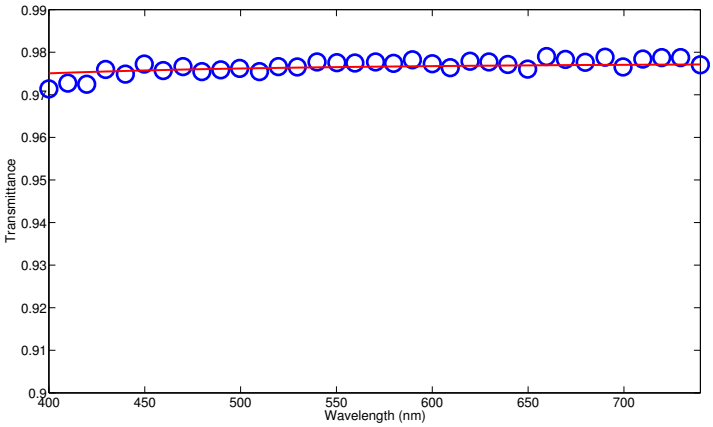
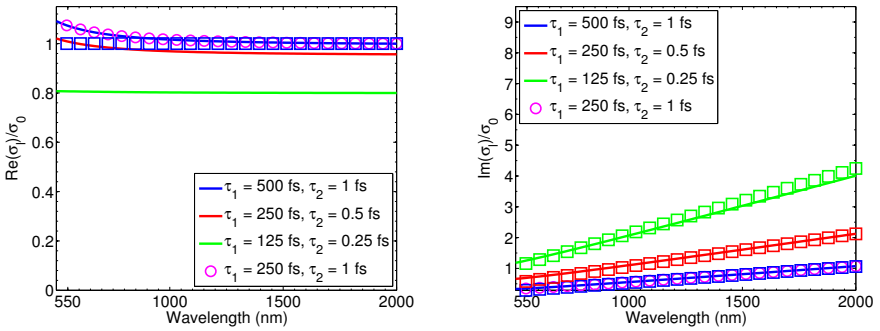


Figure 49: The fitting to the experimental data in [96] by letting $\tau_2 = 0.64$ fs.

ure 50(a) and the imaginary part is plotted in Figure 50(b). They are compared to the analytical solution in Sec. 5.3, whose derivation is based on the ideal Dirac cone assumption. When the wavelength decreases to < 450 nm, the optical conductivity based on the full-band calculation starts to diverge from the analytical solution, resulting in part from the fact that at lower wavelengths, the linear energy dispersion relation becomes invalid. The imaginary part of σ_l mostly depends on the decoherence rate τ_2 [124]. Thus, given the complex optical conductivity experimental measurements from [114–116] at 550 nm, we can extract τ_2 with values ranging from 0.25 fs to 0.72 fs, showing agreement with the previous absorption fitting. With decoherence time less than 0.5 fs, $\tau_1 = 1/\Gamma_1$ begins to decrease. This is because with small decoherence time, the optical linear conductivity becomes significantly different from the universal value $\sigma_0 = e^2/4\hbar$.



(a) The real part of σ_l by setting different τ_1 and τ_2. Solid lines: from full-band calculation. Hollow squares: from the analytical solution in Sec. 5.3.

(b) The imaginary part of σ_l by setting different τ_1 and τ_2. Solid lines: from full-band calculation. Hollow squares: from the analytical solution in Sec. 5.3.

Figure 50: The wavelength dependence of σ_l.

5.3.2 Saturation

Next we will discuss the saturation effect of graphene. With an increasing input power to graphene, more and more electrons are excited from valance band to conduction band. The absorption rate of graphene, which is related to the population inversion

ϱ, decreases due to the fact that fewer electrons can absorb photons and get excited to conduction band. For the two-level model, the saturation effect is well investigated analytically [60] under the rotating-wave approximation, which is valid when the detuning and decay rates are small compared to the optical frequencies. For graphene, the saturation effect is studied semi-classically in [111], resulting in a decay time much shorter than what was measured by differential transmission (DT) experiments [108,125–130]. The proposed quantum model in this thesis can be used to investigate the saturation effect of graphene. Given the intensity of the pump mode I_p the *complex* pump-mode field amplitude can be found by

$$E_p = \sqrt{\frac{I_p}{2\epsilon_0 c}}. \tag{5.3.8}$$

The effective conductivity is defined by Eq. 5.3.7, being a function of τ_1, τ_2, ω_p, and E_p.

The saturation threshold at 800 nm is reported to be 4±1 GW/cm^2 [111]. In Figure 51, The real part of σ_l is plotted with different decay time constants vs. intensity. We also compare the saturation curve obtained by quantum calculations adopted in this thesis with the classical saturation curve given by the nonsaturating optical linear conductivity multiplied by an intensity-dependent coefficient $1/(1 + I/I_{\text{th}})$. At the saturation threshold intensity I_{th}, σ_l is decreased by half. Knowledge of I_{th} and τ_2 allows determination of the carrier-relaxation rate τ_1. In Figure 52 we plot the relation between τ_1 and τ_2 given saturation powers of 3, 4, and 5 GW/cm^2. With τ_2 experimentally obtained from [114–116] and I_{th} obtained by [111], the resulting value of τ_1 ranges from 250 fs to 550 fs, within the range of previously reported DT experimental data [108, 125–130]. The decoherence and carrier-relaxation rate seem to differ from sample to sample. Factors that have impact on the two time constants may also be due to differences in substrate interactions, temperatures, impurities, and/or excitation wavelengths.

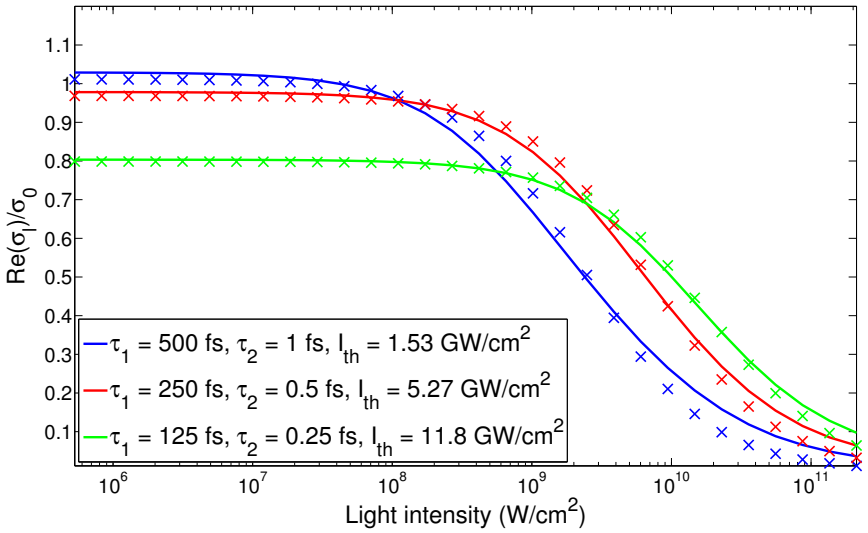


Figure 51: Transmission saturation of the optical conductivity at 1.55 eV (800 nm). Solid lines: from quantum calculations in this thesis. $\times$-marks: fit to classical saturation curve.

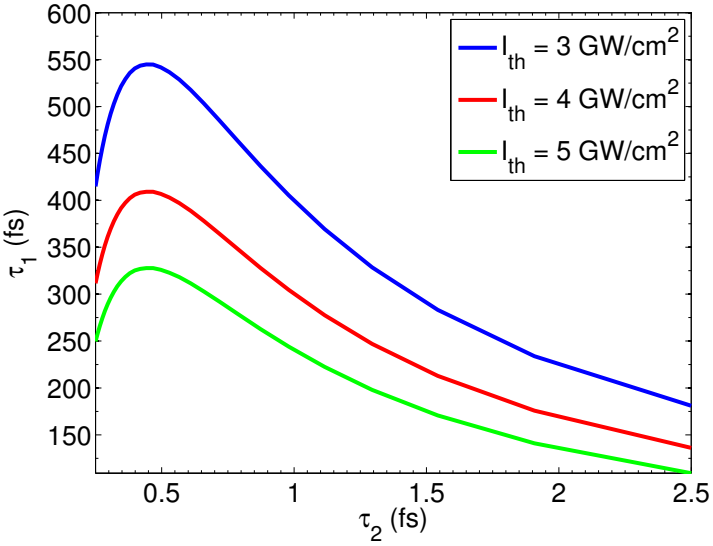


Figure 52: dependence of τ_1 on τ_2 for saturation powers I_{th}. Pump photon energy is 1.55 eV (800 nm).

5.3.3 Nonlinear optical conductivity

For the nonlinear optical conductivity, we focus on co-polarized degenerate four-wave mixing. The FWM conductivity at idler frequency $\omega_i = 2\omega_p - \omega_s$ is defined as

$$\sigma_{\text{FWM}} = 2 \times \frac{8}{3} \times \frac{J^{(2,-1)}}{E_p^2 E_s^*}, \tag{5.3.9}$$

where the coefficient 2 counts the electron spin degeneracy. To compare the nonlinearity of graphene with other normal materials such as glass, the nonlinear optical conductivity $\sigma_{\rm FWM}$ is converted into effective third-order susceptibility by [105]

$$\chi^{(3)}_{\rm eff} = \frac{|\sigma_{\rm FWM}|}{\epsilon_0 \omega_i d}, \tag{5.3.10}$$

where $d \approx 3.3$ Å is the effective thickness of graphene. In Figure 53, we plot the ratio between $\chi^{(3)}_{\rm eff}$ and the third-order susceptibility of glass $\chi^{(3)}_{\rm silica} = 1.84 \times 10^{-22}$ m^2/V^2 at the same wavelength [123]. The full-band calculation is compared with the analytical solution in [124] and with a Lorentzian fit that illustrates the qualitative difference between graphene and a two-level atom, notably graphene's stronger nonlinearity at large detunings. Like the linear optical conductivity σ_l, which saturates with increas-

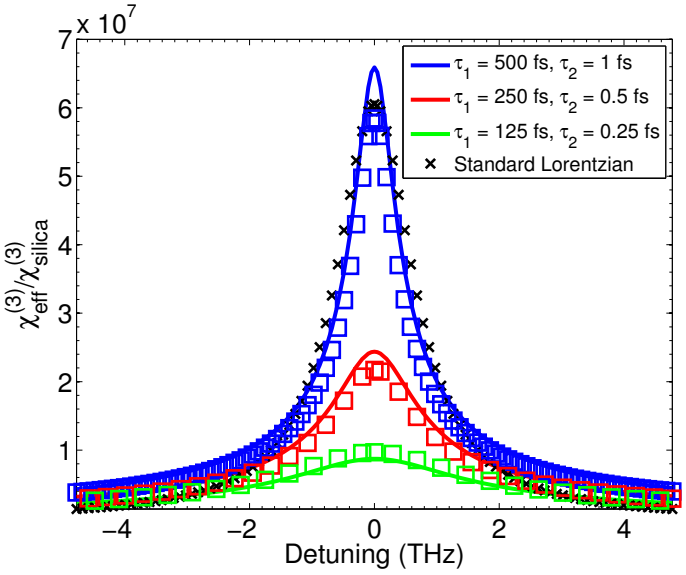


Figure 53: The effective third-order susceptibility of graphene compared to glass. Solid lines: from the full-band calculation. Hollow squares: the analytical solution in Sec. 5.3. ×-marks: a Lorentzian fit to the top blue curve.

ing pump power, the nonlinear optical conductivity also shows a saturation effect. The FWM surface-current density also saturates near 4 GW/cm^2. In Figure 54, saturation of FWM conductivity is plotted. Knowledge of the saturation threshold of FWM in graphene is potentially useful for future FWM experiments with graphene.

We next fit our theory to experimental data obtained by [105]. We use three values

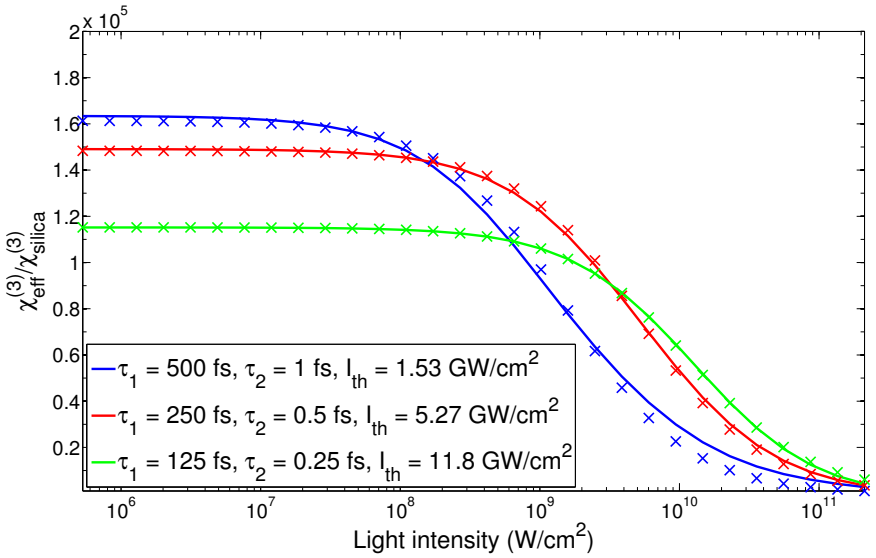


Figure 54: Saturation of the FWM optical conductivity. Pump is at 775 nm and signal is at 1000 nm. Solid lines: from quantum calculations in this thesis. x-marks: fit to classical saturation curve.

for τ_2 found in Sec. 5.2.1 by investigating the imaginary part of the linear complex optical conductivity measured by experiments. Thus, the only parameter to determine is τ_1. Fits to experimental four-wave-mixing data yields τ_1 ranging from 0.8 fs to 1.25 fs. The fits are shown in Figure 55. In the same figure, we also compare our theory with the theory adopted in [105]. To summarize, the decoherence time is taken from linear refractive index measurement, without fitting. Because the amplitude of the nonlinear response is taken directly from the theory and the decoherence time, only one parameter is used to make the fit. The two decay rates were both obtained from experimental data, which provides evidence for ultrafast quantum dephasing in graphene at the 1 fs timescale. Our fully quantum-mechanical model results in faster decay rates than what was reported in [111] based on semi-classical calculations. $\tau_2 \sim 1$ fs is the decoherence rate, which is due to electron-electron scattering. In a low excitation regime like [105], all excited electrons go through an ultrafast thermalization process within 10 fs, which roughly agrees with the τ_1 we found from

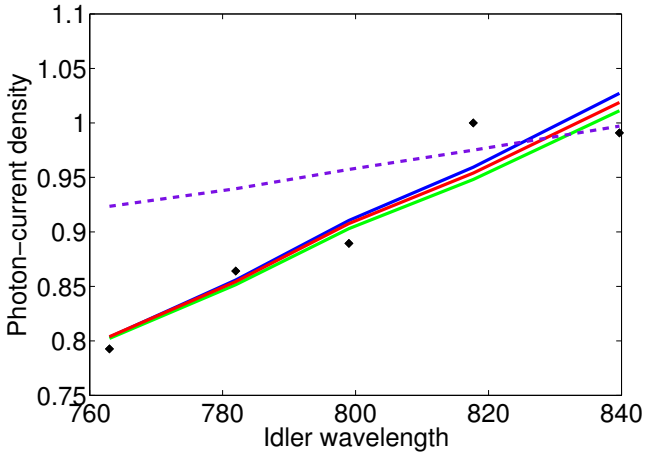


Figure 55: Fitting of the theory to the experimental data obtained by [105]. The two phenomenological decay rates for the three curves are blue: $\tau_1 = 1.25$ fs $\tau_2 = 0.25$ fs; green: $\tau_1 = 1.11$ fs, $\tau_2 = 0.37$ fs; red: $\tau_1 = 0.8$ fs, $\tau_2 = 0.72$ fs. Dashed line: the theory adopted in [105]. Dots: experimental data obtained in [105].

the four-wave mixing experimental data. We need to note here that if we try to fit the first four points instead of entire five points, we get $\tau_1 \sim 10$ fs. Thus, we suggest that accurate experimental measurement of four-wave mixing spectrum is a good probe for these time constants.On the other hand, in a high excitation regime, not all excited electrons can undergo the ultrafast thermalization process, indicating by multiple observed time constants in DT experiments. In this situation, some electrons need phonon-assisted processes to relax. Therefore, τ_1 in high excitation regimes is much longer than 10 fs, which confirms the τ_1 obtained from saturation threshold measurements.

To study the quality of graphene for nonlinear optical experiments, we next investigate its figure of merit defined in [131]:

$$F = \frac{n_2^I I}{\lambda \alpha}, \tag{5.3.11}$$

where

$$n_2^I = \frac{3}{8n^2\epsilon_0 c}\Re(\chi^{(3)}). \tag{5.3.12}$$

In Eq. 5.3.11, we take $\alpha = 7.75 \times 10^7/\text{m}$ as the absorption coefficient of graphene. In the denominator of Eq. 5.3.12, we take $n = 3.0$ as the refractive index of graphene [114]. We then plot the figure of merit of graphene in Figure 56 and compare the figure of merit of graphene with other materials in Table 6.

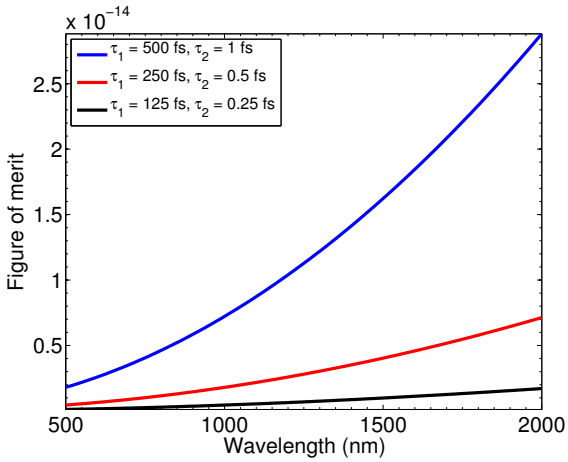


Figure 56: The figure of merit of graphene at different wavelength. The three curves correspond to different time constants.

Table 6: Comparison of figure of merit for different materials. Wavelength is at 1000 nm. Data from [131]

material	**FOM**
GaAlAs (resonant)	1×10^{-8}
GaAlAs (non-resonant)	3.3×10^{-10}
PTS[b] (non-resonant)	5×10^{-13}
silica	1×10^{-11}
graphene	$\sim 1 \times 10^{-14}$

We find that compared to the figure of merit of silica at 1000 nm, the figure of merit of graphene is three orders of magnitude lower. This is due to the fact that graphene is highly absorptive over a wide range of optical wavelengths. However, since graphene does not impose any phase-matching constrain and possesses high large-detuning nonlinearities, it is still a very interesting material for nonlinear optical experiments.

5.4 *Four-wave mixing experiment in graphene*

In this section, our preliminary effort on a four-wave mixing experiment in graphene is described. The graphene sample used in the experiment was grown by expitaxy on a SiC substrate by Dr. Walt de Heer's group in Georgia Tech Atlanta. The number of carbon layers on the Carbon-face is measured to be 15 on average. The experimental schematic is shown in Figure 57.

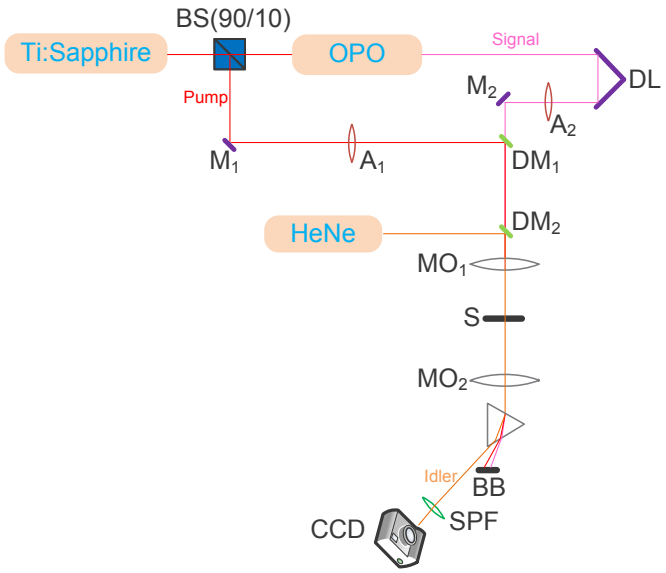


Figure 57: The graphene four-wave mixing experiment schematic. BS: beam-splitter to separate the pump and the input to the OPO. D: delay line. M_1, M_2: mirrors. DM_1, DM_2: dichroic mirrors. MO_1, MO_2: microscopic objectives. A_1, A_2: tunable attenuators. S: the 15-layer graphene sample. BB: beam blocker. SPF: short-pass filter cut-off wavelength 750 nm. CCD: CCD camera to detect the idler. OPO: optical parametric oscillator. HeNe: helium-neon laser serving as a reference beam for the idler.

Now we describe the experimental setup. 200 fs laser pulses at 780 nm are produced by a Ti-sapphire mode-locked laser. A 90/10 beam splitter (BS) separates the total power from the Ti:Sapphire (2 W) into a 200 mW beam, which serves as the pump beam, and a 1.8 W beam for the input of the OPO. A tunable attenuator (A_1) is installed alone the pump path to manipulate the pump power. The output of the

OPO serves as the signal beam and is tuned to 1205 nm so that the idler produced by the graphene sample coincides with the output wavelength on the helium-neon laser (633 nm) if the pump is at 830 nm. The signal-beam power is measured to be 100 mW. The signal is time delayed by a delay line (D) and a mirror (M_2). To control the signal power, another tunable attenuator (A_2) is installed along the signal path. The time-overlapping pump beam and the signal beam are combined co-linearly on a dichroic mirror (DM_1). The signal beam and the pump beam impinge on a with microscopic objective (MO_1) with 6 mm focal length and are focused down to a 10 μm spot. The graphene sample is mounted a stage with x, y, z, and angular degrees of freedom. On the sample, the maximal average power of the pump and the signal is measured to be 150 mW and 30 mW respectively. Taking into account the Ti:sapphire laser repetition rate 76 MHz and the pulse width about 200 fs, it results in a maximal pump peak power density of 12 GW/cm^2 for the pump and 2.5 GW/cm^2 for the signal.

The Rayleigh range of the focused beam can be calculated by

$$z_R = \frac{\pi w^2}{\lambda}, \tag{5.4.1}$$

where w is the beam waist at the focal point, and λ is the wavelength. By substituting $w = 5$ microns and $\lambda = 780$ nm into Eq. 5.4.1, we obtain $z_R \approx 100$ μm. To find the focal point, we set the pump power to 150 mW, resulting in a peak power 12 GW/cm^2. A power meter measures the light coming out from the sample. By adjusting the position of the sample along the z axis, the transmitted light power is stronger when saturation is strong. This allows convenient location of the focal point.

Since the pump beam and the signal beam impinge on the sample normally, the idler beam is expected to be produced perpendicular to the sample surface. The transmitted pump, signal, and idler beams go through another microscopic objective (MO_2). A prism is installed to spatially separate the three beams. The pump beam and the signal beam are blocked by a beam blocker. The idler beam is guided to

two short-pass filters with cut-off wavelength at 750 nm. The idler beam is finally detected by a CCD camera.

To locate the idler beam, an auxiliary helium-neon (HeNe) laser severs as a reference beam if the pump is tuned to 830 nm. The visible beam from the HeNe laser transmits through the center of MO_1 and impinges on the sample perpendicularly at the focal point. The idler beam is expected to follow the path of the reference beam.

Once the sample is placed on the focal point, we try to measure the idler power as a function of the pump power. We fix the signal power at 1 mW and vary the pump power from 10 mW to 100 mW, resulting in a power excitation power density from 0.8 GW/cm^2 to 8 GW/cm^2. We exploit a quadratic fit to confirm the four-wave mixing. We find that besides the quadratic contribution from four-wave mixing, a linear contribution also exists. We believe this linear contribution comes from leaked pump photons. It requires better filtering to further suppress pump photons leaked to the detection system. However, in the experimental scheme where the pump wavelength is at 780 nm, we expect that most four-wave mixing is produced by the silicon carbide substrate since the pump photon energy is at the half bandgap of silicon carbide. We have currently tuned the pump wavelength to 830 nm, which is off resonant for silicon carbide, and expect the four-wave mixing from the substrate to be 20 dB lower than pumping it at 780 nm. We are still working on the optical alignment and hope to collect experimental data soon.

A successful four-wave mixing experiment in graphene would allow us to probe the decay-time constant τ_1 and τ_2 and confirm graphene's large nonlinearity for future applications in micro-fabricated quantum-communication devices.

CHAPTER VI

CONCLUSIONS

This chapter summarizes the main contributions of this thesis. Efforts under investigation or proposed for future work will also be summarized.

6.1 Main contributions

The main accomplishments of this thesis include:

- A theoretical proposal of a continuous-variable quantum key distribution (CVQKD) protocol. The proposed CVQKD protocol is compatible with high-rate operation. In particular, it loosens the efficiency requirement on error-correction codes, leading to the utilization of codes almost two orders of magnitude faster than those used in competing protocols, while still operating in a secure region.

- An experimental demonstration of the proposed CVQKD protocol. The experiment is not only the first discrete-signaling CVQKD demonstration in fiber, but also the first experimental implementation of a CVQKD system with a continuous-wave local oscillator (CWLO). Excess noise caused by scattering from the CWLO is avoided by a frequency-shift scheme. The quadrature probability distribution of the GAWBS noise is measured by quantum tomographic measurements. Statistical tests show strong evidence of Gaussian probability distributions of the field quadratures, which validate the security calculations done in the protocol for typical operating conditions.

- An experimental implementation of an ultrafast quantum random-number generator based on amplified spontaneous emission (ASE). The throughput of the quantum random-number generator is 20 Gbit/s. The produced random bits

passed the NIST random-number tests. A theoretical study discussing the ultimate limits on the performance of ASE based random-number generators is also performed. Theoretical results find performance limits of the randomness source used in the experiment.

- Development of a quantum-dynamical theory of nonlinear optical interactions, in particular four-wave mixing, in graphene. The theory predicts the complex linear optical conductivity, the saturation threshold, and the nonlinear optical conductivity of graphene, showing agreement with various reported experimental data.

- A four-wave mixing experiment in graphene.

6.2 Future work

Based on the accomplishments of this thesis, several research topics under investigation and future research areas are listed as follows:

- An analysis on the data-size effect on QKD. Statistical fluctuations, which occur with limited amounts of collected data, may influence the security of QKD protocols. A rigorous treatment on the data-size effect is needed.

- A QKD experiment in which the signal is frequency shifted beyond 2 GHz and detected by a high-bandwidth photon detector. The new implementation is more straightforward than the frequency-shift scheme in described in this thesis.

- Cryptographically, random numbers produced by the ultrafast quantum-random generator can be utilized in a different way. By designing new classical cryptographic protocols using large amount of true-random numbers, it might be possible tie a security proof to NP-complete problems. Compared to quantum cryptography, classical cryptographic protocols can be implemented more

efficiently and with lower cost.

- A quantum-dynamic theory dealing with pulsed laser signals interacting with graphene. In the pulsed-based theory, phenomenological decay constants need to be treated differently, and a fully quantum-mechanical examination is desired.

- Twin-photon production based on four-wave mixing in graphene. Coincidence-based photon-counting techniques are needed to verify twin-photon production.

APPENDIX A

NUMERICAL SIMULATION TECHNIQUES

It is difficult to obtain analytical solutions for continuous variable quantum states, because they have infinite dimension. Unlike the protocols based on Gaussian modulation of signal, discrete modulation only gives *conditional* Gaussian states instead of global Gaussian states. If the global state, such as $\hat{\rho}_E$, is not Gaussian, it is difficult to find an analytical solution for its von Neumann entropy if excess noise is introduced into the channel. Fortunately, as long as the excess noise is weak, it is still possible to obtain numerical solutions.

From Eq. (3.1.23), one may see that if Eve's two mode quantum state is expanded in Fock space, there would be infinite number of terms. But one may truncate the state into a finite number of terms because when τ is small, the amplitudes for large photon numbers are so small that they are negligible. For this simulation, we have the excess noise about 0.005 of one shot-noise unit and this leads to $\tau = 0.033$ for 25 km and $\tau = 0.0167$ for 50 km. Using only the first three terms of the expansion is then justified. In other words, the terms up to 2 photons are preserved. We let EMAX = 2 denoting the maximal number of photons.

Now we can approximate Eve's two-mode state as

$$|\Psi_{\varepsilon_n,\varepsilon_r}\rangle = \sqrt{1-\tau^2}\sum_{n=0}^{\mathrm{EMAX}} \tau^n |n\rangle_{\varepsilon_n}|\phi(n)\rangle_{\varepsilon_r}. \tag{A.0.1}$$

The mode ε_n is interacted with the mode a. However, since the quantum state in the mode ε_n is represented in Fock space, it needs to be transformed into coherent form so that the operation of BS_1 is performed on two coherent states, making the its output coherent states for numerical convenience. Here we use an approximation

where $|n\rangle$ is represented as the superposition of $n+1$ coherent states [132]:

$$|n,r\rangle = c(r)\frac{\sqrt{n!}e^{\frac{r^2}{2}}}{(n+1)r^n}\sum_{k=0}^{n} e^{\frac{2\pi i}{n+1}k}|re^{\frac{2\pi i}{n+1}k}\rangle, \tag{A.0.2}$$

where $c(r)$ is used to normalize $|n,r\rangle$. We have

$$|n,r\to 0\rangle = |n\rangle. \tag{A.0.3}$$

The accuracy of the approximation is

$$1-|c_n|^2 = \frac{n!}{(2n+1)!}r^{2(n+1)} + o(r^{4(n+1)}), \tag{A.0.4}$$

where $|c_n|^2$ is the probability of $|n\rangle$ being $|n,r\rangle$. In practice, we set $r=0$ for $|0\rangle$ and $r=0.1$ for other Fock states.

Thus, we write $|\Phi\rangle$ as

$$\begin{aligned}|\Phi\rangle \;=\; & c(r)\sqrt{1-\tau^2}\sum_{j=1}^{4}\frac{1}{2}|j\rangle_{a'}\sum_{n=0}^{\mathrm{EMAX}}\tau^n|n\rangle_{\varepsilon_r}\frac{\sqrt{n!}e^{\frac{(r_n)^2}{2}}}{(n+1)(r_n)^n}\\ & \times\sum_{k=0}^{n}e^{\frac{2\pi ik}{n+1}}|\sqrt{\eta_m}(\sqrt{\eta}\alpha_j+\sqrt{1-\eta}r_n e^{\frac{2\pi ik}{n+1}})\rangle_{b'}\\ & \times|\sqrt{1-\eta_m}(\sqrt{\eta}\alpha_j+\sqrt{1-\eta}r_n e^{\frac{2\pi ik}{n+1}})\rangle_{\mathrm{hom}}|\sqrt{1-\eta}\alpha_j-\sqrt{\eta}r_n e^{\frac{2\pi ik}{n+1}}\rangle_{\varepsilon'_n}\end{aligned} \tag{A.0.5}$$

.

We first trace over the mode a' to get the density matrix of mode b', ε'_n, ε_r, and hom:

$$\hat{\rho}_{b',\varepsilon'_n,\varepsilon_r,\mathrm{hom}} = \mathrm{Tr}_{a'}(|\Phi\rangle\langle\Phi|) = \sum_{i=1}^{4}\frac{1}{4}|\Omega_i\rangle\langle\Omega_i|, \tag{A.0.6}$$

The density matrix for the mode b', ε'_n, ε_r, and hom is mixed by 4 different pure states $|\Omega_i\rangle$, resulting from Alice's photon-counting measurement on the mode a'. This exactly corresponds to the case in which Alice prepares one of the four coherent states and sends it to Bob. For each of the $|\Omega_i\rangle$, Bob makes a homodyne measurement on his mode b'. The outcome of the homodyne measurement is a Gaussian distributed continuous random variable with average value $u_i = \Re(\sqrt{\eta\eta_m}\alpha_i)$ and variance V_S.

Physically, for each of the $|\Omega_i\rangle$, Bob's measurement outcome has infinite possibilities. However, only the values close to u_i occur with high possibility. As an approximation, our simulation only takes the value in the range $\left[u_i - 6\sqrt{V_S}, u_i + 6\sqrt{V_S}\right]$. Another approximation is that instead of processing the continuous data in the range $\left[u_i - 6\sqrt{V_S}, u_i + 6\sqrt{V_S}\right]$, we divide it into XMAX bins with equal widths and assume that that Bob's measurement only has approximately XMAX different outcomes instead of infinite possibilities. Suppose each bin left bounded by $lb_{i,k}$, and right bounded by $rb_{i,k}$, where $1 \leq k \leq \text{XMAX}$. The measurement result $X_{i,k} = (lb_{i,k} + rb_{i,k})/2$ is obtained with probability $p(X_{i,k}) = \frac{1}{\sqrt{2\pi V_S}} \int_{lb_{i,k}}^{rb_{i,k}} \exp(-\frac{(x-u_i)^2}{2V_S})dx$. The density matrix $\hat{\rho}_{\varepsilon_n,\varepsilon_r,\text{hom}}$ is approximated as

$$\begin{aligned}
\hat{\rho}_{\varepsilon'_n,\varepsilon_r,\text{hom}} = \text{Tr}_{b'}(\hat{\rho}_{b',\varepsilon'_n,\varepsilon_r,\text{hom}}) &= \sum_{i=1}^{4} \frac{1}{4} \sum_{k=1}^{\text{XMAX}} p(X_{i,k}) \frac{\langle X_{i,k}|\Omega_i\rangle\langle\Omega_i|X_{i,k}\rangle}{\langle\Omega_i|X_{i,k}\rangle\langle X_{i,k}|\Omega_i\rangle} \\
&= \sum_{i=1}^{4} \frac{1}{4} \sum_{k=1}^{\text{XMAX}} p(X_{i,k}) |\psi_{i,k}\rangle\langle\psi_{i,k}|, \qquad \text{(A.0.7)}
\end{aligned}$$

where $|\psi_{i,k}\rangle = \frac{\langle X_{i,k}|\Omega_i\rangle}{\sqrt{\langle\Omega_i|X_{i,k}\rangle\langle X_{i,k}|\Omega_i\rangle}}$. To evaluate $\hat{\rho}_E$, we need to trace $|\psi^{i,k}\rangle\langle\psi^{i,k}|$ over mode hom. For low signal-to-noise ratios, the mean photon number in mode hom is low. If we use Fock basis to expand mode hom, we can neglect the quantum states with large photon numbers. Suppose we express mode hom in Fock space and only keep the states up to HMAX photons, we have

$$\text{Tr}_{\text{hom}}(\hat{\rho}^{i,k}_{\varepsilon'_n,\varepsilon_r,\text{hom}}) = \sum_{j=0}^{\text{HMAX}} {}_{\text{hom}}\langle j|\psi_{i,k}\rangle\langle\psi_{i,k}|j\rangle_{\text{hom}}. \qquad \text{(A.0.8)}$$

It turns out that

$$\begin{aligned}
\hat{\rho}_E &= \sum_{i=1}^{4} \frac{1}{4} \sum_{k=1}^{\text{XMAX}} p(X_{i,k}) \sum_{j=0}^{\text{HMAX}} \langle j|\psi_{i,k}\rangle\langle\psi_{i,k}|j\rangle \\
&= \sum_{i=1}^{4} \frac{1}{4} \sum_{k=1}^{\text{XMAX}} p(X_{i,k}) \sum_{j=0}^{\text{HMAX}} p(j|X_{i,k}) |\epsilon_{i,j,k}\rangle\langle\epsilon_{i,j,k}|, \qquad \text{(A.0.9)}
\end{aligned}$$

where $|\epsilon_{i,j,k}\rangle = \frac{\langle j|\psi_{i,k}\rangle}{\sqrt{\langle\psi_{i,k}|j\rangle\langle j|\psi_{i,k}\rangle}}$ and $p(j|X_{i,k}) = \langle\psi_{i,k}|j\rangle\langle j|\psi_{i,k}\rangle$, where we have ignored the subscript for $|j\rangle_{\text{hom}}$. If we define a global probability $p(|\epsilon_{i,j,k}\rangle) = \frac{1}{4}p(X_{i,k})p(j|X_{i,k})$,

we can rewrite $\hat{\rho}_E$ as

$$\hat{\rho}_E = \sum_{i,j,k} p(|\epsilon_{i,j,k}\rangle)|\epsilon_{i,j,k}\rangle\langle\epsilon_{i,j,k}|, \tag{A.0.10}$$

where we have ignored the subscript E. The problem of calculating the von Neumann entropy $S(\hat{\rho}_E)$ is equivalent to solving the eigenvalue of the corresponding Gram matrix [133]. Each element of the Gram matrix is

$$G_{ijk,i'j'k'} = \sqrt{p(|\epsilon_{i,j,k}\rangle)p(|\epsilon_{i',j',k'}\rangle)}\langle\epsilon_{i,j,k}|\epsilon_{i',j',k'}\rangle. \tag{A.0.11}$$

The non-zero eigenvalues of G equal the non-zero eigenvalues of $\hat{\rho}_E$. Suppose the non-zero eigenvalues of G are $\{\lambda_1, \lambda_2, ..., \lambda_n\}$, we have

$$S(\hat{\rho}_E) = \sum_{i=1}^{n} -\lambda_i \log_2(\lambda_i). \tag{A.0.12}$$

We next examine $p(|\epsilon_{i,j,k}\rangle|q=1)$, used to evaluate $S(\hat{\rho}_{E|q=1})$. We first reformulate $p(|\epsilon_{i,j,k}\rangle|q=1)$ by Bayes' theorem:

$$p(|\epsilon_{i,j,k}\rangle|q=1) = \frac{p(q=1||\epsilon_{i,j,k}\rangle)p(|\epsilon_{i,j,k}\rangle)}{p(q=1)}. \tag{A.0.13}$$

The first term on the numerator is evaluated by

$$p(q=1||\epsilon_{i,j,k}\rangle) = \frac{\frac{1}{\sqrt{2\pi V_S}}\int_{lb_{i,k}}^{rb_{i,k}} \exp\left[-\frac{(x-u_i)^2}{2V_S}\right] \frac{1}{\sqrt{2\pi V_{\rm el}}}\int_0^{\infty} \exp\left[-\frac{(y-x)^2}{2V_{\rm el}}\right] dydx}{\frac{1}{\sqrt{2\pi V_S}}\int_{lb_{i,k}}^{rb_{i,k}} \exp\left[-\frac{(x-u_i)^2}{2V_S}\right] dx}. \tag{A.0.14}$$

Since $\hat{\rho}_{E|q=1} = \sum_{i,j,k} p(|\epsilon_{i,j,k}\rangle|q=1)|\epsilon_{i,j,k}\rangle\langle\epsilon_{i,j,k}|$, we can calculate $S(\hat{\rho}_{E|q=1})$ following the Gram-matrix method.

For the post-selection case, we need to evaluate $p(|\epsilon_{i,j,k}\rangle|q\neq 0)$, which is rewritten by Bayes' theorem:

$$p(|\epsilon_{i,j,k}\rangle|q\neq 0) = \frac{p(q\neq 0||\epsilon_{i,j,k}\rangle)p(|\epsilon_{i,j,k}\rangle)}{p(q\neq 0)}. \tag{A.0.15}$$

The first term on the numerator is obtained by

$$\begin{aligned} p(q \neq 0||\epsilon_{i,j,k}\rangle) &= \frac{1}{\frac{1}{\sqrt{2\pi V_S}}\int_{lb_{i,k}}^{rb_{i,k}} \exp\left[-\frac{(x-u_i)^2}{2V_S}\right] dx} \\ &\times \frac{1}{\sqrt{2\pi V_S}}\int_{lb_{i,k}}^{rb_{i,k}} \exp\left[-\frac{(x-u_i)^2}{2V_S}\right] \\ &\times \frac{1}{\sqrt{2\pi V_{\rm el}}}\left(\int_{-\infty}^{-T} \exp\left[-\frac{(y-x)^2}{2V_{\rm el}}\right] + \int_{T}^{\infty} \exp\left[-\frac{(y-x)^2}{2V_{\rm el}}\right]\right) dydx. \end{aligned} \tag{A.0.16}$$

Again, $S(\hat{\rho}_E)$ is evaluated by the Gram-matrix method.

In order to calculate $S(\hat{\rho}_{E|q=1})$ for the case with post selection, we need to calculate the probability $p(|\epsilon_{i,j,k}\rangle|q=1)$. We first rewrite it by Bayes' theorem in Eq. (A.0.13). However, now the first term on the numerator must be calculated differently by

$$p(q=1||\epsilon_{i,j,k}\rangle) = \frac{\frac{1}{\sqrt{2\pi V_S}}\int_{lb_{i,k}}^{rb_{i,k}} \exp\left[-\frac{(x-u_i)^2}{2V_S}\right] \frac{1}{\sqrt{2\pi V_{\rm el}}}\int_{T}^{\infty} \exp\left[-\frac{(y-x)^2}{2V_{\rm el}}\right] dydx}{\frac{1}{\sqrt{2\pi V_S}}\int_{lb_{i,k}}^{rb_{i,k}} \exp\left[-\frac{(x-u_i)^2}{2V_S}\right] dx}. \tag{A.0.17}$$

Finally, we obtain $\hat{\rho}_{E|q=1}$, based on which $S(\hat{\rho}_{E|q=1})$ is evaluated.

To demonstrate the accuracy of our numerical simulation results, we first compare it with the analytical solution in the limit of no excess noise. We choose $\tau = 1 \times 10^{-6}$ in our numerical simulation, showing that the difference in ΔI is only 6.5804×10^{-7} bits between the numerical and the analytical result.

In the end, we make a comparison of the different results by setting different parameters, i.e., EMAX, XMAX, HMAX, and r_k. We find that for EMAX > 2, XMAX > 20, HMAX > 6, and $r_k < 0.1$, only tiny different among different numerical simulations exists. We believe that the simulation results are accurate enough for these parameters.

The simulation results with different parameters are shown in Table 7. We take the secret-key capacity obtained at 25 km without post selection by setting EMAX $= 2$, XMAX $= 20$, HMAX $= 6$, and $r = 0.1$ as the reference and mark it as $\Delta I_{\rm ref}$. We give

Table 7: Differences of the secret-key capacity with ΔI_{ref}. Here 25 km denotes the case of 25 km QIQO CVQKD without post-selection. 25 km-ps denotes the case of 25 km QIQO CVQKD with post-selection. 50 km denotes the case of 50 km QIQO CVQKD without post-selection. 50 km-ps denotes the case of 50 km QIQO CVQKD with post-selection.

	$\overline{\lvert\Delta I_{\mathrm{ref}} - \Delta I_*\rvert}$			
	25 km	25 km-ps	50 km	50 km-ps
$\Delta I_{\mathrm{XMAX}=10}$	7.35×10^{-5}	9.97×10^{-5}	4.25×10^{-5}	1.04×10^{-4}
$\Delta I_{\mathrm{XMAX}=30}$	4.58×10^{-6}	5.84×10^{-6}	1.93×10^{-6}	5.46×10^{-6}
$\Delta I_{r=0.5}$	5.89×10^{-5}	4.01×10^{-4}	4.54×10^{-5}	3.50×10^{-3}
$\Delta I_{r=0.05}$	2.98×10^{-6}	8.23×10^{-6}	1.51×10^{-6}	9.42×10^{-5}
$\Delta I_{\mathrm{EMAX}=1}$	2.63×10^{-6}	2.42×10^{-5}	9.85×10^{-7}	9.78×10^{-5}
$\Delta I_{\mathrm{EMAX}=3}$	1.31×10^{-7}	5.60×10^{-7}	3.83×10^{-10}	1.22×10^{-8}
$\Delta I_{\mathrm{HMAX}=4}$	1.41×10^{-5}	3.16×10^{-5}	1.51×10^{-6}	9.42×10^{-5}
$\Delta I_{\mathrm{HMAX}=8}$	5.22×10^{-8}	9.26×10^{-8}	1.28×10^{-12}	7.28×10^{-12}

the difference of ΔI_* with the reference. ΔI_* is obtained by setting parameters other than those used for ΔI_{ref}. We record $\overline{\lvert\Delta I_{\mathrm{ref}} - \Delta I_*\rvert}$ in Table 7.

Table 7 shows that if we set EMAX = 2, XMAX = 20, HMAX = 6, and $r = 0.1$, we are close enough to the exact solution because if we further adjust the parameters, the result only changes by a tiny bit. For the final results, we set EMAX = 3, XMAX = 30, HMAX = 8, and $r = 0.05$. We believe that these parameters give us numerical simulation results that are extremely close to the exact solutions.

REFERENCES

[1] G.E. Moore et al. Cramming more components onto integrated circuits. *Proceedings of the IEEE*, 86(1):82–85, 1998.

[2] D. Stinson. *Cryptography: Theory and practice*. CRC press, 2002.

[3] A.K. Lenstra and H.W. Lenstra. *The development of the number field sieve*, volume 1554. Springer, 1993.

[4] S.A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the third annual ACM symposium on Theory of computing*, pages 151–158. ACM, 1971.

[5] T. Baker, J. Gill, R. Solovay, S.A. Kurtz, S.R. Mahaney, and J.S. Royer. Relativizations of the P =? NP question. *Journal of the ACM*, 42:401–420, 1975.

[6] A.A. Razborov and S. Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24–35, 1997.

[7] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir. Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. *Advances in Cryptology–EUROCRYPT 2010*, pages 299–319, 2010.

[8] M.A. Nielsen, I. Chuang, and L.K. Grover. Quantum computation and quantum information. *American Journal of Physics*, 70:558, 2002.

[9] A.D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[10] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. Bangalore, India, 1984.

[11] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin. Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6):2515–2534, 2008.

[12] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology*, pages 10–18. Springer, 1985.

[13] A.K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[14] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 70(13):1895, 1993.

[15] H.J. Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, 2008.

[16] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71:1675, 2000.

[17] J.F. Dynes, Z.L. Yuan, A.W. Sharpe, and A.J. Shields. A high speed, post-processing free, quantum random number generator. *Applied Physics Letters*, 93:031109, 2008.

[18] S.K. Tawfeeq. A random number generator based on single-photon avalanche photodiode dark counts. *Journal of Lightwave Technology*, 27(24):5665–5667, 2009.

[19] P. Bronner, A. Strunz, C. Silberhorn, and J.P. Meyn. Demonstrating quantum random with single photons. *European Journal of Physics*, 30:1189, 2009.

[20] C. Suematsu, N. Namekata, I. Shimada, and S. Inoue. Generation of physical random numbers by means of photon counting. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 90(2):1–8, 2007.

[21] M.A. Wayne, E.R. Jeffrey, G.M. Akselrod, and P.G. Kwiat. Photon arrival time quantum random number generation. *Journal of Modern Optics*, 56(4):516–522, 2009.

[22] G.E. Katsoprinakis, M. Polis, A. Tavernarakis, A.T. Dellis, and I.K. Kominis. Quantum random number generator based on spin noise. *Physical Review A*, 77(5):054101, 2008.

[23] B. Qi, Y.M. Chi, H.K. Lo, and L. Qian. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Optics Letters*, 35(3):312–314, 2010.

[24] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U.L. Andersen, C. Marquardt, and G. Leuchs. A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, 2010.

[25] Y. Shen, L. Tian, and H. Zou. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Physical Review A*, 81(6):063814, 2010.

[26] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh. An optical ultrafast random bit generator. *Nature Photonics*, 4(1):58–61, 2009.

[27] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter. Ultrahigh-speed random number generation based on a chaotic semiconductor laser. *Physical Review Letters*, 103(2):24102, 2009.

[28] Y. Yamanashi and N. Yoshikawa. Superconductive random number generator using thermal noises in SFQ circuits. *IEEE Transactions on Applied Superconductivity*, 19(3):630–633, 2009.

[29] C.S. Calude, M.J. Dinneen, M. Dumitrescu, and K. Svozil. Experimental evidence of quantum randomness incomputability. *Physical Review A*, 82(2):022102, 2010.

[30] M. Fiorentino, C. Santori, S.M. Spillane, R.G. Beausoleil, and W.J. Munro. Secure self-calibrating quantum random-bit generator. *Physical Review A*, 75(3):032334, 2007.

[31] T. Sugiura, Y. Yamanashi, and N. Yoshikawa. Statistical evaluation of a superconductive physical random number generator. *IEICE Transactions on Electronics*, 93(4):453–457, 2010.

[32] K. Svozil. Three criteria for quantum random-number generators based on beam splitters. *Physical Review. A*, 79(5):054306, 2009.

[33] P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, and Y. Shih. New high-intensity source of polarization-entangled photon pairs. *Physical Review Letters*, 75(24):4337–4341, 1995.

[34] J.G. Rarity and P.R. Tapster. Experimental violation of Bell's inequality based on phase and momentum. *Physical Review Letters*, 64(21):2495–2498, 1990.

[35] J. Brendel, E. Mohler, and W. Martienssen. Experimental test of Bell's inequality for energy and time. *EPL (Europhysics Letters)*, 20:575, 1992.

[36] L. Gordon, G.L. Woods, R.C. Eckardt, R.R. Route, R.S. Feigelson, M.M. Fejer, and R. Byer. Diffusion-bonded stacked GaAs for quasiphase-matched second-harmonic generation of a carbon dioxide laser. *Electronics Letters*, 29(22):1942–1944, 1993.

[37] A. Galvanauskas, D. Harter, M.A. Arbore, M.H. Chou, and M.M. Fejer. Chirped-pulse-amplification circuits for fiber amplifiers, based on chirped-period quasi-phase-matching gratings. *Optics Letters*, 23(21):1695–1697, 1998.

[38] S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, P. Baldi, M. DeMicheli, D.B. Ostrowsky, and N. Gisin. PPLN waveguide for quantum communication. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, 18(2):155–160, 2002.

[39] K.L. Vodopyanov, O. Levi, P.S. Kuo, T.J. Pinguet, J.S. Harris, M.M. Fejer, B. Gerard, L. Becouarn, and E. Lallier. Optical parametric oscillation in quasi-phase-matched GaAs. *Optics Letters*, 29(16):1912–1914, 2004.

[40] K. Sanaka, K. Kawahara, and T. Kuga. New high-efficiency source of photon pairs for engineering quantum entanglement. *Physical Review Letters*, 86(24):5620–5623, 2001.

[41] K. Banaszek, A.B. U'Ren, and I.A. Walmsley. Generation of correlated photons in controlled spatial modes by downconversion in nonlinear waveguides. *Optics Letters*, 26(17):1367–1369, 2001.

[42] X. Li, P.L. Voss, J.E. Sharping, and P. Kumar. Optical-fiber source of polarization-entangled photons in the 1550 nm telecom band. *Physical Review Letters*, 94(5):53601, 2005.

[43] M. Fiorentino, P.L. Voss, J.E. Sharping, and P. Kumar. All-fiber photon-pair source for quantum communications. *IEEE Photonics Technology Letters*, 14(7):983–985, 2002.

[44] X. Li, J. Chen, P.L. Voss, J. Sharping, and P. Kumar. All-fiber photon-pair source for quantum communications: Improved generation of correlated photons. *Optics Express*, 12(16):3737–3744, 2004.

[45] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N.J. Cerf, R. Tualle-Brouri, S.W. McLaughlin, and P. Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A*, 76(4):042305, 2007.

[46] W.A. De Heer, C. Berger, X. Wu, et al. Epitaxial graphene. *Solid state communications*, 143(1-2):92–100, 2007.

[47] I. Csiszár and J. Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[48] U.M. Maurer. Secret key agreement by public discussion from common information. *Information Theory, IEEE Transactions on*, 39(3):733–742, 1993.

[49] A.S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[50] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301, 2009.

[51] F. Grosshans. Collectiveattacks and unconditional security in continuous variable quantum key distribution. *Physical Review Letters*, 94(2):20504, 2005.

[52] M. Navascués and A. Acín. Security bounds for continuous variables quantum key distribution. *Physical Review Letters*, 94(2):20505, 2005.

[53] R. García-Patrón and N.J. Cerf. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters*, 97(19):190503, 2006.

[54] M. Navascués, F. Grosshans, and A. Acin. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Physical Review Letters*, 97(19):190502, 2006.

[55] Y.B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Physical Review A*, 79(1):012307, 2009.

[56] M. Heid and N. Lütkenhaus. Security of coherent-state quantum cryptography in the presence of Gaussian noise. *Physical Review A*, 76(2):022313, 2007.

[57] A. Leverrier and P. Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical review letters*, 102(18):180504, 2009.

[58] R. Renner and J.I. Cirac. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Physical review letters*, 102(11):110504, 2009.

[59] R. Shankar. *Principles of quantum mechanics*. Springer, 1994.

[60] R.W. Boyd. *Nonlinear optics*. Academic Pr, 1992.

[61] H. Haug and S.W. Koch. *Quantum theory of the optical and electronic properties of semiconductors*. World Scientific Pub Co Inc, 2004.

[62] F. Grosshans and P. Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables. *Arxiv preprint quant-ph/0204127*, 2002.

[63] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5):57902, 2002.

[64] R. Namiki and T. Hirano. Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection. *Physical Review A*, 74(3):032302, 2006.

[65] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. A framework for practical quantum cryptography. *Reviews of Modern Physics*, 81, 2008.

[66] C. Silberhorn, T.C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Physical Review Letters*, 89(16):167901, 2002.

[67] C. Weedbrook, A.M. Lance, W.P. Bowen, T. Symul, T.C. Ralph, and P.K. Lam. Coherent-state quantum key distribution without random basis switching. *Physical Review A*, 73(2):022316, 2006.

[68] A.M. Lance, T. Symul, V. Sharma, C. Weedbrook, T.C. Ralph, and P.K. Lam. No-switching quantum key distribution using broadband modulated coherent light. *Physical review letters*, 95(18):180503, 2005.

[69] T. Symul, D.J. Alton, S.M. Assad, A.M. Lance, C. Weedbrook, T.C. Ralph, and P.K. Lam. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise. *Physical Review A*, 76(3):030303, 2007.

[70] J. Singh, O. Dabeer, and U. Madhow. Capacity of the discrete-time AWGN channel under output quantization. In *IEEE International Symposium on Information Theory*, pages 1218–1222. IEEE, 2008.

[71] V. Buzek and G. Drobny. Quantum tomography via the maxent principle. *Journal of Modern Optics, 47*, 14(15):2823–2839, 2000.

[72] R. Ahlswede and P. Löber. Quantum data processing. *IEEE Transactions on Information Theory*, 47(1):474–478, 2001.

[73] A. Khandekar and R.J. McEliece. On the complexity of reliable communication on the erasure channel. In *Proceeding of IEEE International Symposium on IEEE International Symposium on Information Theory*, page 1. IEEE, 2001.

[74] Z.S. Zhang and P.L. Voss. A path towards 10 Gb/s continuous-variable quantum key distribution. In *LPHYS08*. Trondheim, Norway, July 2008.

[75] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier. Field test of a continuous-variable quantum key distribution prototype. *New Journal of Physics*, 11:045023, 2009.

[76] B. Qi, L.L. Huang, L. Qian, and H.K. Lo. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Physical Review A*, 76(5):052323, 2007.

[77] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier. Quantum key distribution using Gaussian-modulated coherent states. *Nature*, 421(6920):238, 2003.

[78] S. Lorenz, N. Korolkova, and G. Leuchs. Continuous-variable quantum key distribution using polarization encoding and post selection. *Applied Physics. B, Lasers and Optics*, 79(3):273–277, 2004.

[79] A.J. Poustie. Guided acoustic-wave Brillouin scattering with optical pulses. *Optics Letters*, 17(8):574–576, 1992.

[80] A. Leverrier, F. Grosshans, and P. Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6):062343, 2010.

[81] Z.S. Zhang and P.L. Voss. Security of a discretely signaled continuous variable quantum key distribution protocol for high rate systems. *Optics express*, 17(14):12090–12108, 2009.

[82] P.L. Voss, K.G. Köprülü, and P. Kumar. Raman-noise-induced quantum limits for $\chi^{(3)}$ nondegenerate phase-sensitive amplification and quadrature squeezing. *Journal of the Optical Society of America B*, 23(4):598–610, 2006.

[83] G.P. Agarwal. Nonlinear fiber optics. *Acad. Press, New York*, 1995.

[84] Q. Dinh Xuan, Z.S. Zhang, and P.L. Voss. A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Optics Express*, 17(26):24244–24249, 2009.

[85] D. Levandovsky, M. Vasilyev, and P. Kumar. Near-noiseless amplification of light by a phase-sensitive fibre amplifier. *Pramana*, 56(2):281–285, 2001.

[86] K. Bergman, H.A. Haus, E.P. Ippen, and M. Shirasaki. Squeezing in a fiber interferometer with a gigahertz pump. *Optics Letters*, 19(4):290–292, 1994.

[87] A.J. Poustie. Bandwidth and mode intensities of guided acoustic-wave Brillouin scattering in optical fibers. *Journal of the Optical Society of America B*, 10(4):691–696, 1993.

[88] W.S. Wong, H.A. Haus, L.A. Jiang, P.B. Hansen, and M. Margalit. Photon statistics of amplified spontaneous emission noise in a 10-Gbit/s optically preamplified direct-detection receiver. *Optics Letters*, 23(23):1832–1834, 1998.

[89] C.R.S. Williams, J.C. Salevan, X. Li, R. Roy, and T.E. Murphy. Fast physical random number generator using amplified spontaneous emission. *Optics Express*, 18(23):23584–23597, 2010.

[90] Z.S. Zhang, Q. Dinh Xuan, and P.L. Voss. A provably secure streamcipher based on a high-speed quantum random number generator. In *Frontier in Optics*. Rochester, USA, October 2010.

[91] A.H. Castro Neto, F. Guinea, N.M.R. Peres, K.S. Novoselov, and A.K. Geim. The electronic properties of graphene. *Reviews of modern physics*, 81:109–162, 2009.

[92] KS Novoselov, AK Geim, SV Morozov, D. Jiang, Y. Zhang, SV Dubonos, IV Grigorieva, and AA Firsov. Electric field effect in atomically thin carbon films. *Science*, 306(5696):666, 2004.

[93] C. Berger, Z. Song, T. Li, X. Li, A.Y. Ogbazghi, R. Feng, Z. Dai, A.N. Marchenkov, E.H. Conrad, N. Phillip, et al. Ultrathin epitaxial graphite: 2D electron gas properties and a route toward graphene-based nanoelectronics. *The Journal of Physical Chemistry B*, 108(52):19912–19916, 2004.

[94] X. Du, I. Skachko, A. Barker, and E.Y. Andrei. Approaching ballistic transport in suspended graphene. *Nature Nanotechnology*, 3(8):491–495, 2008.

[95] V.P. Gusynin and S.G. Sharapov. Transport of Dirac quasiparticles in graphene: Hall and optical conductivities. *Physical Review B*, 73(24):245411, 2006.

[96] R.R. Nair, P. Blake, A.N. Grigorenko, K.S. Novoselov, T.J. Booth, T. Stauber, N.M.R. Peres, and A.K. Geim. Fine structure constant defines visual transparency of graphene. *Science*, 320(5881):1308, 2008.

[97] T. Stauber, N.M.R. Peres, and A.K. Geim. Optical conductivity of graphene in the visible region of the spectrum. *Physical Review B*, 78(8):085432, 2008.

[98] M. Mecklenburg, J. Woo, and B.C. Regan. Tree-level electron-photon interactions in graphene. *Physical Review B*, 81(24):245401, 2010.

[99] D. Harter and R. Boyd. Nearly degenerate four-wave mixing enhanced by the ac Stark effect. *IEEE Journal of Quantum Electronics*, 16(10):1126–1131, 1980.

[100] SA Mikhailov. Non-linear electromagnetic response of graphene. *EPL (Europhysics Letters)*, 79:27002, 2007.

[101] SA Mikhailov and K. Ziegler. Nonlinear electromagnetic response of graphene: frequency multiplication and the self-consistent-field effects. *Journal of Physics: Condensed Matter*, 20:384204, 2008.

[102] B. Rosenstein, M. Lewkowicz, H.C. Kao, and Y. Korniyenko. Ballistic transport in graphene beyond linear response. *Physical Review B*, 81(4):041416, 2010.

[103] B. Dóra and R. Moessner. Nonlinear electric transport in graphene: Quantum quench dynamics and the Schwinger mechanism. *Physical Review B*, 81(16):165431, 2010.

[104] K.L. Ishikawa. Nonlinear optical response of graphene in time domain. *Physical Review B*, 82(20):201402, 2010.

[105] E. Hendry, P.J. Hale, J. Moger, A.K. Savchenko, and SA Mikhailov. Coherent nonlinear optical response of graphene. *Physical Review Letters*, 105(9):97401, 2010.

[106] D. Bauer, D.B. Milošević, and W. Becker. Strong-field approximation for intense-laser–atom processes: The choice of gauge. *Physical Review A*, 72(2):023415, 2005.

[107] M. Lewkowicz and B. Rosenstein. Dynamics of particle-hole pair creation in graphene. *Physical Review Letters*, 102(10):106802, 2009.

[108] D. Sun, Z.K. Wu, C. Divin, X. Li, C. Berger, W.A. de Heer, P.N. First, and T.B. Norris. Ultrafast relaxation of excited Dirac fermions in epitaxial graphene using optical differential transmission spectroscopy. *Physical Review Letters*, 101(15):157402, 2008.

[109] T. Winzer, A. Knorr, and E. Malic. Carrier multiplication in graphene. *Nano Letters*, 10(12):4839–4843, 2010.

[110] S. Piscanec, M. Lazzeri, F. Mauri, A.C. Ferrari, and J. Robertson. Kohn anomalies and electron-phonon interactions in graphite. *Physical Review Letters*, 93(18):185503, 2004.

[111] G. Xing, H. Guo, X. Zhang, T.C. Sum, and C.H. Huan. The physics of ultrafast saturable absorption in graphene. *Optics Express*, 18(5):4564, 2010.

[112] H.C. Kao, M. Lewkowicz, and B. Rosenstein. Ballistic transport, chiral anomaly, and emergence of the neutral electron-hole plasma in graphene. *Physical Review B*, 82(3):035406, 2010.

[113] M. Kira and SW Koch. Many-body correlations and excitonic effects in semiconductor spectroscopy. *Progress in Quantum Electronics*, 30(5):155–296, 2006.

[114] M. Bruna and S. Borini. Optical constants of graphene layers in the visible range. *Applied Physics Letters*, 94(3):031901–031901, 2009.

[115] X. Wang, Y.P. Chen, and D.D. Nolte. Strong anomalous optical dispersion of graphene: Complex refractive index measured by picometrology. *Optics Express*, 16(26):22105–22112, 2008.

[116] Z.H. Ni, H.M. Wang, J. Kasim, H.M. Fan, T. Yu, Y.H. Wu, Y.P. Feng, and Z.X. Shen. Graphene thickness determination using reflection and contrast spectroscopy. *Nano Letters*, 7(9):2758–2763, 2007.

[117] H.S. Skulason, P.E. Gaskell, and T. Szkopek. Optical reflection and transmission properties of exfoliated graphite from a graphene monolayer to several hundred graphene layers. *Nanotechnology*, 21:295709, 2010.

[118] R.W. Boyd, M.G. Raymer, P. Narum, and D.J. Harter. Four-wave parametric interactions in a strongly driven two-level system. *Physical Review A*, 24(1):411, 1981.

[119] J. Nilsen and A. Yariv. Nondegenerate four-wave mixing in a doppler-broadened resonant medium. *Journal of the Optical Society of America A*, 71(2):180–183, 1981.

[120] A. Zumbusch, G.R. Holtom, and X.S. Xie. Three-dimensional vibrational imaging by coherent anti-Stokes Raman scattering. *Physical Review Letters*, 82(20):4142–4145, 1999.

[121] C.W. Freudiger, W. Min, B.G. Saar, S. Lu, G.R. Holtom, C. He, J.C. Tsai, J.X. Kang, and X.S. Xie. Label-free biomedical imaging with high sensitivity by stimulated Raman scattering microscopy. *Science*, 322(5909):1857, 2008.

[122] G.P. Agrawal. *Nonlinear fiber optics (third edition)*. Academic Press, 2001.

[123] D. Milam. Review and assessment of measured values of the nonlinear refractive-index coefficient of fused silica. *Applied optics*, 37(3):546–550, 1998.

[124] Z.S. Zhang and P.L. Voss. A quantum-dynamical theory for nonlinear optical interactions in graphene. *Arxiv preprint arXiv:1106.4838*, 2011.

[125] J.M. Dawlaty, S. Shivaraman, M. Chandrashekhar, F. Rana, and M.G. Spencer. Measurement of ultrafast carrier dynamics in epitaxial graphene. *Applied Physics Letters*, 92:042116, 2008.

[126] X. Zhao, Z.B. Liu, W.B. Yan, Y. Wu, X.L. Zhang, Y. Chen, and J.G. Tian. Ultrafast carrier dynamics and saturable absorption of solution-processable few-layered graphene oxide. *Applied Physics Letters*, 98:121905, 2011.

[127] M. Breusing, C. Ropers, and T. Elsaesser. Ultrafast carrier dynamics in graphite. *Physical Review Retters*, 102(8):86809, 2009.

[128] M. Breusing, S. Kuehn, T. Winzer, E. Malić, F. Milde, N. Severin, J.P. Rabe, C. Ropers, A. Knorr, and T. Elsaesser. Ultrafast nonequilibrium carrier dynamics in a single graphene layer. *Physical Review B*, 83(15):153410, 2011.

[129] P.J. Hale, S.M. Hornett, J. Moger, D.W. Horsell, and E. Hendry. Hot phonon decay in supported and suspended exfoliated graphene. *Physical Review B*, 83(12):121404, 2011.

[130] F. Carbone, G. Aubock, A. Cannizzo, F. Van Mourik, RR Nair, AK Geim, KS Novoselov, and M. Chergui. Femtosecond carrier dynamics in bulk graphite and graphene paper. *Chemical Physics Letters*, 504:37–40, 2011.

[131] AG Astill. Material figures of merit for non-linear optics. *Thin solid films*, 204(1):1–17, 1991.

[132] J. Janszky, P. Domokos, S. Szabo, and P. Adam. Quantum-state engineering via discrete coherent-state superpositions. *Physical Review A*, 51:4191–4193, 1995.

[133] R. Jozsa and J. Schlienz. Distinguishability of states and von neumann entropy. *Physical Review A*, 62(1):012301, 2000.

New techniques for quantum communication systems

Zheshen Zhang

154 Pages

Directed by Professor Paul L. Voss

Although mathematical cryptography has been widely used, its security has only been proven under certain assumptions such as the computational power of opponents. As an alternative, quantum communication, in particular quantum key distribution (QKD) does not require unproven assumptions and can achieve unconditional security. However, the key-generation rate of practical QKD systems is limited by device imperfections, excess noise from the quantum channel, a limited rate of true random-number generation, limited rate of quantum entanglement preparation, and/or high complexity of post-processing. This dissertation contributes to improved performance of quantum communication systems. First, it proposes a new continuous-variable QKD (CVQKD) protocol that loosens the efficiency requirement on post-processing, a bottleneck for long-distance CVQKD systems. It also demonstrates an experimental implementation of the proposed protocol. To allow for future higher rate implementation, the CVQKD experiment uses a continuous-wave local oscillator (CWLO). The excess noise caused by guided acoustic-wave Brillioun scattering (GAWBS) is avoided by a frequency-shift scheme. The statistical distribution of GAWBS noise is characterized by quantum tomography. Measurements show Gaussian statistics with 55 dB of dynamic range, which validate efficient security calculations used in the proposed CVQKD protocol. True random numbers are required in quantum and classical cryptography. A second contribution of this thesis is that it experimentally demonstrates an ultrafast quantum random-number generator (QRNG) based on amplified spontaneous emission (ASE). Random numbers are produced by a multi-mode photon counting measurement on ASE light. The performance of the QRNG is analyzed with quantum information theory and tested

with NIST standard random-number test. The QRNG experiment demonstrates a random-number generation rate at 20 Gbit/s. A theoretical study identifies show fundamental limits for such QRNGs. Quantum entanglement produced in nonlinear optical processes can help to increase quantum communication distance. A third contribution is research of the nonlinear optics of graphene, a novel 2D material with unconventional physical properties. Based on a quantum-dynamical model, the optical response of graphene is derived, showing a link between the complex linear optical conductivity and the decoherence. Nonlinear optical response, in particular four-wave mixing, is studied for the first time. The theory predicts saturation effects in graphene and relates the saturation threshold to phenomenologically model ultrafast decoherence and carrier relaxation in graphene. Experimental efforts towards validation of this theory are discussed.